



# Feature at a Glance

## Ability to audit security-related activity in SAP Ariba

Andy Rubinson, SAP Ariba  
Target GA: August, 2021

CONFIDENTIAL

# Feature at a Glance

Ease of implementation  High-touch  
Geographic relevance  Global

## Introducing: Ability to audit security-related activity in SAP Ariba

### Customer challenge

Security incidents are a constant threat in today's world, but more administrative tools are needed to help diagnose them and take necessary actions and countermeasures. Without a well-documented logging of business events and alerting of potential issues taking place, customers are open to increased security risk and financial loss.

### Solution area

SAP Ariba Buying  
SAP Ariba Buying and Invoicing  
SAP Ariba Commerce Automation  
SAP Ariba Commerce Automation Membership  
SAP Ariba Contract Invoicing  
SAP Ariba Contracts  
SAP Ariba Catalog  
SAP Ariba Discount Management  
SAP Ariba Invoice Management  
SAP Ariba Sourcing  
SAP Ariba Spend Analysis  
SAP Ariba Spot Buy Catalog  
SAP Ariba Payables  
SAP Ariba Strategic Sourcing Suite  
SAP Ariba Supplier Information and Performance Management  
SAP Ariba Supplier Lifecycle and Performance  
SAP Ariba Supplier Risk  
SAP Ariba Supply Chain Collaboration for Buyers

### Meet that challenge with SAP Ariba

This feature introduces the SAP Ariba audit service, which logs selected user and administration actions performed in SAP Ariba applications. You can use the SAP Ariba audit service to monitor security-related system information such as:

- changes to user records
- changes to application data
- changes to application configurations

It also helps security personnel reproduce potential malicious activities of users and administrators, monitor administrative activities, like configuration changes, and retrieve forensic evidence if a security breach occurs.

### Implementation information

This feature is automatically on for all customers with the applicable solutions but requires **customer configuration**.

**Note:** This feature is being enabled in phases started with US and EU data centers. Customers on other data centers will be notified when the feature is available.

### Experience key benefits

Having a well-established logging of business events will help in analyzing the activities and identify any malicious activities within the system. Well logged business events will also provide forensic evidence in case of a breach, allowing customers to properly investigate security incidents.

### Prerequisites and Restrictions

You must be a member of the Customer Administrator or Audit User group to access the SAP Ariba audit service.

The SAP Ariba audit service is available in the Intelligent Configuration Manager workspace in the Ariba Administrator.

The SAP Ariba audit service does not log cryptographic information that can be used to access or authenticate users or data, such as passwords, shared secrets, private keys, or tokens.

The SAP Ariba audit service logs cannot be modified.

## Feature at a Glance

# Introducing: Ability to audit security-related activity in SAP Ariba

Select the search filters, or enter search criteria and click **Apply** to narrow the search results.

### Search filter options:

- Event type
- Application
- User
- From
- To
- Action
- Event category
- Operation
- Attributes
- Document ID
- Document type

Home Buying and Invoicing Privacy Management **Audit Log**

### Audit events and reports


Events Reports

#### Search filters

Event type *	Application	User	From *	To		
Select one ▼	Select one ▼		mm/dd/yyyy 📅	mm/dd/yyyy 📅		
Action	Event category	Operation	Attributes	Document ID	Document type	
Select one ▼	Select one ▼					

Fewer options ^

Reset filters Apply



Use the search filters to search for specific audit events.

Export results

## Feature at a Glance

# Introducing: Ability to audit security-related activity in SAP Ariba

## Search: Filter Options and descriptions

Filter	Description
<b>Event type</b>	The type used for categorizing the logged event. This is a required search filter. For example, use <b>Security</b> to view security critical events. Use <b>Data access</b> to view data access related activities. For more information about event types, refer to <a href="#">Audit event types</a> .
<b>Application</b>	The application from where the event is generated.
<b>User</b>	The name of the user who actually performed the action.
<b>From</b>	The start date for the event filter. This is a required search filter. You can choose a valid date (within the last 3 months) using the calendar tool.
<b>To</b>	The end date for the event filter. You can choose a valid date (within the last 3 months) using the calendar tool.
<b>Action</b>	The action associated with the event. For example, Login, Logout, Insert, Update, Delete, and so on.
<b>Event category</b>	The category of the events you want to view. For example, PII, PCI, Business critical, and Security event.
<b>Operation</b>	The operation that initiated the audit event. For example, File upload, Password reset, Failed login, and so on.
<b>Attributes</b>	The additional attributes of the event.
<b>Document ID</b>	The ID of the document that was modified.
<b>Document type</b>	The type of document that was modified. For example, Requisition, Order Receipt, and so on.

# Feature at a Glance

## Introducing: Ability to audit security-related activity in SAP Ariba

### Enter search criteria


Home   Buying and Invoicing   Privacy Management   **Audit Log**

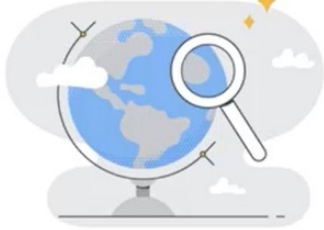
#### Audit events and reports

Events   Reports

##### Search filters

<b>Event type *</b> Security	Application Select one	User 	<b>From *</b> 05/01/2021	To mm/dd/yyyy	
Action Select one	Event category Select one	Operation 	Attributes 	Document ID 	Document type 

[Fewer options ^](#)   



Use the search filters to search for specific audit events.

[Export results](#)

# Feature at a Glance

## Introducing: Ability to audit security-related activity in SAP Ariba

View the search results in the table

### Results include:

- Event ID
- Date
- Event Type
- Application
- User
- From
- To
- Action
- Event category
- Operation
- Attributes
- Document ID
- Document type

The screenshot displays a search interface for SAP Ariba. At the top, there are several filter fields: 'Event type \*' (set to Security), 'Application' (Select one), 'User' (empty), 'From \*' (05/01/2021), and 'To' (mm/dd/yyyy). Below these are 'Action' (Select one), 'Event category' (Select one), 'Operation' (empty), 'Attributes' (empty), 'Document ID' (empty), and 'Document type' (empty). There are 'Reset filters' and 'Apply' buttons. A 'Fewer options ^' link is also present. Below the filters is a 'Search results' section with a search bar. The results are shown in a table with the following data:

Event ID	Date	Event type	User	Effective user	Action	Applicat
DBPeTF	2021-04-30T14:20:...	Security	superuser	customersupportadmin	AUTHENTICATION	Buyer
DBPeS5	2021-04-30T14:20:...	Security	ghalas	ghalas	LOGIN	Buyer
DBPeS6	2021-04-30T14:20:...	Security	ghalas	ghalas	LOGIN	Buyer
DBPeTQ	2021-04-30T14:20:...	Security	ghalas	ghalas	LOGOUT	Buyer
DBPeS7	2021-04-30T14:20:...	Security	ghalas	ghalas	AUTHENTICATION	Buyer
DBPv5G	2021-05-01T01:02:...	Security	adavis	adavis	LOGIN	Buyer
DBPv5H	2021-05-01T01:02:...	Security	adavis	adavis	LOGIN	Buyer
DBPv5I	2021-05-01T01:02:...	Security	adavis	adavis	AUTHENTICATION	Buyer

An 'Export results' button is located at the bottom right of the table.

## Feature at a Glance

Introducing: **Ability to audit security-related activity in SAP Ariba**

### Create report from search results

- Enter desired filter and **Apply**
- Select **Export results** to create report

The screenshot shows the SAP Ariba search results interface. At the top, there are filter fields for Action, Event category, Operation, Attributes, Document ID, and Document type. The 'Attributes' field is highlighted with a red box and contains the value 'IsNonPO'. A red arrow points from this field to the 'Apply' button. Below the filters, there is a search bar and a table of search results. A red arrow points from the 'Export results' button at the bottom right of the table back to the 'Apply' button. The table has columns for Format, Status, Source service, Document status, System request, Trace ID, and Description. The results show a list of active documents with a system request of false.

Format	Status	Source service	Document status	System request	Trace ID	Description
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...
			Active	false		Object of type 'ariba.invoici...



# Feature at a Glance

## Introducing: Ability to audit security-related activity in SAP Ariba

### Create report from search results

- Screen moves from Events tab to Reports tab
- Notifications of report in progress
- Report appears in reports list

The screenshot displays the SAP Ariba interface. At the top, the 'Reports' tab is selected, indicated by a red arrow. A notification box at the top right states: 'Audit report DataModification\_2021-06-17 is in progress. This process may take a few minutes. Please check back again later.' Below this, the 'Search filters' section includes dropdowns for 'Event type' and 'Application', and date pickers for 'From' and 'To'. A 'Reset filters' button and an 'Apply' button are also present. The main area shows a table of 'Audit reports' with columns for Report name, Created by, Created date, Event type, Status, and Action. The first row, 'DataModification\_2021-06-17', is highlighted, and a red arrow points to its 'PENDING' status. The other two rows, 'test' and 'test-icm', are in 'PURGED' status. A 'Create report' button is visible at the bottom right.

Report name	Created by	Created date	Event type	Status	Action
DataModification_2021-06-17	John Ham	Jun 17 2021, 10:43:11 AM, GMT+05:30	DataModification	PENDING	<a href="#">Download</a>
test	Chad Noll	Jun 10 2021, 8:34:43 AM, GMT+05:30	DataModification	PURGED	<a href="#">Download</a>
test-icm	Chad Noll	Jun 10 2021, 5:16:45 AM, GMT+05:30	DataModification	PURGED	<a href="#">Download</a>



# Feature at a Glance

## Introducing: Ability to audit security-related activity in SAP Ariba

### View and filter reports

- Assign search filters on:
  - Event type
  - Application
  - Date
- Apply filter

The screenshot displays the 'Audit Log' section of the SAP Ariba interface. The main heading is 'Audit events and reports'. Below this, there are tabs for 'Events' and 'Reports'. The 'Search filters' section includes dropdown menus for 'Event type' and 'Application', and date pickers for 'From' and 'To'. A 'Reset filters' button and an 'Apply' button are also present. A table below the filters shows audit events with columns for 'Created by', 'Created date', 'Event type', 'Status', and 'Action'. A 'Create report' button is located at the bottom right.

	Created by	Created date	Event type	Status	Action
<a href="#">report 1</a>	John Ham	Jun 17 2021, 10:48:11 AM, GMT+05:30	GenericAction	PROCESSING	<a href="#">Download</a>
<a href="#">Demo report 1</a>	John Ham	Jun 17 2021, 10:45:39 AM, GMT+05:30	DataModification	COMPLETED	<a href="#">Download</a>
<a href="#">DataModification_2021-06-17</a>	John Ham	Jun 17 2021, 10:43:11 AM, GMT+05:30	DataModification	COMPLETED	<a href="#">Download</a>

Follow us



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/copyright](http://www.sap.com/copyright) for additional trademark information and notices.

**THE BEST RUN**

