



November 9, 2021

# Why is Security Audit Logging Important?

Presented by Isaac Kimmel, Senior Product Manager

For SAPSA Use Only



START

---



# Agenda

- Introduction
- What is the security audit log?
- Why does it matter?
- Practical considerations
- Software integration
- Summary
- Q&A

# Introduction

Name: Isaac Kimmel

Role: Senior Product Manager

Email: [ikimmel@securityweaver.com](mailto:ikimmel@securityweaver.com)

I began working with SAP in 2005 as part of a Basis and Security team for a big four consulting firm. Over the past decade, I have worked with many Security Weaver customers all over the world for implementation and training. I also work as a training class instructor.

# What is the SAL?

The Security Audit Log (SAL) is used to record security related system information. The SAL is intended to capture detailed information that can later be reviewed by team members (or auditors) as needed.

For SAPSA Use Only

# Why use it?

Generally, it is recommended to activate and use the SAL to ensure detailed data is available – especially if a security incident or risk occurs.

Gain visibility into sensitive (audit log) events that occur in the system.

For example:

- activities of critical system users (SAP\*, DDIC)
- failed user login attempts

# Reason #1 – SAL Usage is Required!

It is very likely that usage of the Security Audit Log has been required in your organization from an audit and/or compliance perspective.

Basic SAL functionality should already be activated in your systems – especially production systems.

For SAPSA Use Only

For SAPSA Use Only

# Example events from the SAL

- Debugging (change mode)
- Generic table access using transactions like SE16, SE16N, SM30, SM31, SM34, or SQV
- File downloads

For SAPSA Use Only



# Reason #2 – Critical Information in the SAL

Critical information **can and should** be logged! The SAL provides unique capabilities in this regard.  
Do not assume this information is being captured elsewhere.

If you wait until an incident occurs, it is too late!



For SAPSA Use Only

For SAPSA Use Only

# SAL Configuration

- Transaction SM19
- Activate filters for specific (or all) users
- Select the events (message IDs) to be logged
- Make sure to discuss or review the retention policy – how long will the log files be available?

For SAPSA Use Only



The screenshot displays the SAP SAL configuration interface. At the top, there are two tabs: "Filter 1" (selected) and "Filter 2". Below the tabs, there is a checkbox labeled "Filter active" which is checked. To the right of this checkbox are two buttons: "Reset" and "Detailed Display". Below these elements is a "Selection criteria" section. It contains a "Client" field with an asterisk, a radio button selected for "User Name", and two unselected radio buttons for "User Group (Incl.)" and "User Group (Excl.)". At the bottom of this section is a "User ID" field with an asterisk.

For SAPSA Use Only

# SAL Configuration - Example

- Grouping by criticality is provided

For SAPSA Use Only

Detailed View of Audit Events to Be Recorded (Filter 1)				
Audit Class	Event Cla...	Recordi...	Message ID	System log message text (before setting variables)
Dialog Logon	Critical	<input checked="" type="checkbox"/>	AU2	Logon failed (reason=&B, type=&A, method=&C)
Dialog Logon		<input type="checkbox"/>	AUM	User &B Locked in Client &A After Erroneous Password Checks
Dialog Logon		<input type="checkbox"/>	AUN	User &B in Client &A Unlocked After Being Locked Due to Inval.Password Ente
Dialog Logon		<input type="checkbox"/>	BUD	WS: Delayed logon failed (type &B, WP &C). Refer to Web service log &A.
Dialog Logon		<input type="checkbox"/>	BUE	WS: Delayed logon successful (type &B, WP &C). Refer to Web service log &A
Dialog Logon		<input type="checkbox"/>	BUI	SPNego replay attack detected (UPN=&A)
Dialog Logon		<input type="checkbox"/>	CU4	OAuth 2.0: Logged-on client user &A not same as parameter client ID &B
Dialog Logon		<input type="checkbox"/>	CU6	OAuth 2.0: Client ID &A in SAML assertion not same as client ID &B in request
Dialog Logon		<input type="checkbox"/>	DU0	Invalid SAP GUI data

For SAPSA Use Only

# SAL Reporting

- Transaction SM20
- Enter selection criteria and click “Reread Audit Log” button to execute report

Analysis of Security Audit Log

Reread Audit Log

System Application Server Audit Log Entries Read 0

Time Period Restriction

From Date/Time 08/16/2021 / 12:00:00

To Date/Time 08/16/2021 /

Events Extras Format Statistic

Reset Detail Sel.

Selection Criteria	Audit Classes	Events
Client *	<input checked="" type="checkbox"/> Dialog Logon	All
User *	<input checked="" type="checkbox"/> RFC/CPIC Logon	
	<input checked="" type="checkbox"/> RFC Call	
	<input checked="" type="checkbox"/> Transaction Start	
	<input checked="" type="checkbox"/> Report start	
	<input checked="" type="checkbox"/> User master change	
	<input checked="" type="checkbox"/> Other events	
	<input checked="" type="checkbox"/> System Events	

For SAPSA Use Only

For S

# SAL Reporting - Example

- Default layout shown

Creation Date	Date/Time	Cl.	User Name	Terminal	Transaction Code	Program	Audit Log Msg. Text	L...	Proc.	WP	Variable Message Data
08/09/2021	12:45:14	800	DREINSMA	SWDIA...	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P )	D	014	A	
08/09/2021	13:47:43	800	ACHRISTIAN	AsokX1	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P )	D	011	A	
08/09/2021	21:52:04	800	GGAUTAM	Ggauta...	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P )	D	011	A	
08/09/2021	21:52:09	800	GGAUTAM	Ggauta...	SESSION_MANAGER	SAPMSYST	Logon failed (reason=1, type=A, method=P )	D	011	A	
08/09/2021	22:48:55	800	VMARRIPUDI	Venkat...	/PSYNG/PA	/PSYNG/SA_ITC05	Field content changed: appended line to table LT_PH[]	D	017		appended line to table LT_PH[]
08/09/2021	22:48:55	800	VMARRIPUDI	Venkat...	/PSYNG/PA	/PSYNG/SA_ITC05	Field content changed: LT_PH[8]-PH_NAME -> [S:RULE_ID]	D	017		LT_PH[8]-PH_NAME -> [S:RULE_ID]
08/09/2021	22:49:36	800	VMARRIPUDI	Venkat...	/PSYNG/PA	/PSYNG/SA_ITC05	Field content changed: LT_PH[9]-PH_NAME -> [S:RULE_DESCRIPTION]	D	017		LT_PH[9]-PH_NAME -> [S:RULE_DESCRIPTION]
08/09/2021	22:49:36	800	VMARRIPUDI	Venkat...	/PSYNG/PA	/PSYNG/SA_ITC05	Field content changed: appended line to table LT_PH[]	D	017		appended line to table LT_PH[]
08/09/2021	23:47:57	800	MMEHTO	Mmeht...	/PSYNG/TA	/PSYNG/BC_USRHIS_32	Field content changed: appended line to table OT_DHUC00[]	D	013		appended line to table OT_DHUC00[]
08/09/2021	23:47:57	800	MMEHTO	Mmeht...	/PSYNG/TA	/PSYNG/BC_USRHIS_32	Field content changed: OT_DHUC00[1]-ACCOUNT -> mmehto	D	013		OT_DHUC00[1]-ACCOUNT -> mmehto
08/09/2021	23:50:32	800	MMEHTO	Mmeht...	/PSYNG/TA	/PSYNG/BC_USRHIS_32	Field content changed: <STATS>-TCODE -> /SAP/BC/APC/SAP/WEBGUI_SERVICES	D	013		<STATS>-TCODE -> /SAP/BC/APC/SAP/WEBGUI_SERVICES
08/10/2021	00:57:15	800	VMARRIPUDI	Venkat...	SE38	/PSYNG/SA_SCAN	Field content changed: <WA_RFC>-RFCDEST -> T64CLNT800	D	002		<WA_RFC>-RFCDEST -> T64CLNT800

For SAPSA Use Only

# Reason #3 – Improve Insight

Take advantage of the SAL data you already have! Gain additional insight and context for user behavior or sensitive events in your system(s).

For example:

- High number of failed logins for a specific user ID (or from a specific Terminal)
- Unexpected debugging activities – any debugging access should be granted via emergency access process (and/or solution), yet matching date/time cannot be found.

For SAPSA Use Only

For SAPSA Use Only

# Practical considerations for the SAL

- Are the logs retained online for long term access? Are they archived off after 90 days?
- Who can access the reporting? Are file downloads used to provide the information to other team members?
- Do the logs actually get looked at on a regular basis? Or only if an incident occurs?
- Provided reporting is very focused and intended for a limited audience e.g. Basis team



- Consider leveraging SAL data in other ways
  - Custom spreadsheets
  - Custom dashboards
  - Other software may be able to consume this data
- Goal = expedite timely review of critical information and expand SAL relevant use cases

For SAPSA Use Only

# Consumption of SAL data by other software

Software that can consume and display the SAL data can help increase the visibility of the logged information and allow additional use cases.

Security Weaver's **Transaction Archive** (TA) release 2.8 supports SAL integration!



For SAPSA Use Only

For SAPSA Use Only

# TA 2.8 SAL Benefits

Long term retention of key SAL data (indefinite)

- Eliminates concern about data retention and archiving

Deeper unified view of user behavior (TA history + changes + SAL)

- No time spent creating a spreadsheet from multiple data sources

SAL events included in Sensitive Actions email alerts for proactive notifications

- Designated team can be notified based on event e.g. file downloads

# Example TA Reporting

**Please contact Security Weaver for a demonstration!**

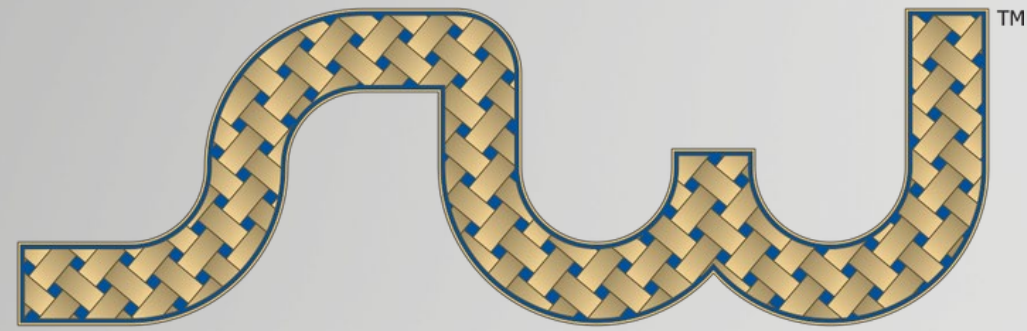
For SAPSA Use Only

For SAPSA Use Only

# SUMMARY AND Q&A

- The Security Audit Log should be activated and used in your system(s)
- Proactively review the SAL configuration with your team to ensure critical events (to your organization) are being logged
- Utilize the SAL data to gain insight and improve context
- Go beyond the basics – use software to build on the SAL foundation

# Contact Us



SECURITY WEAVER

## Mailing Address

3400 N 1200 W Suite 201 Lehi, UT 84043

## Email Address

[info@securityweaver.com](mailto:info@securityweaver.com)

## Phone number

(800) 620-4210

