SAP Innovative Business Solutions
Make Innovation Real

Security Webcast for SAP User Groups

SAP UI Data Protection: Take “crown jewel” protection to the next level

Tobias Keller, Deepak Gupta, Arun Verma – Product Management, SAP

March, 2022

THE BEST RUN SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP.
Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

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, which speak only as of their dates,
and they should not be relied upon in making purchasing decisions.

Agenda

1

Use cases
Solution overview

2

Product demo

3

Roadmap

4

Q & A

Business Needs

addressed by the SAP UI Data Protection suite

1 **Manage access to sensitive data across the organization to…**

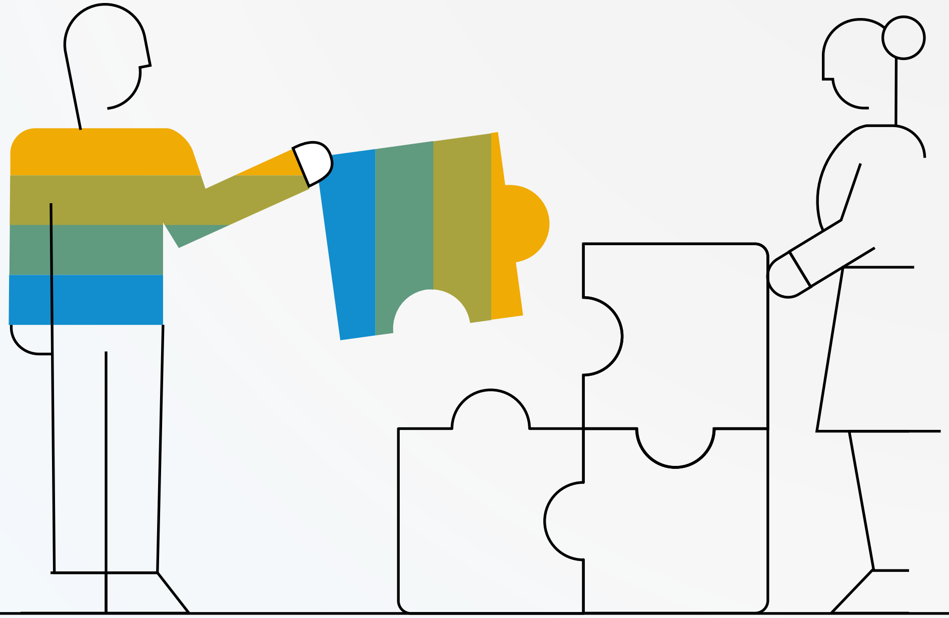
- safeguard business-critical operations
- prevent data leaks and misuse by internal employees

2 **Get insight on data access activities to…**

- understand user behaviors and interpret intentions
- decide on the best course of action

3 **Keep an audit trail of data access to…**

- comply with increasing regulatory and business requirements
- provide evidence during an investigation



Protecting data on the UI layer: two step approach

UI Data Security: two step approach to protect data from insiders

UI Masking

conceal specific data – unless required for tasks

➔ make sensitive data unavailable for data abuse

UI Logging

keep data accessible – and create a broad + deep log of data access

➔ induce compliant behavior

➔ identify & prove irregular data usage

Lock it…

…or log it!

Scenarios

Regulatory, legislative & compliance

Demergers/spin-offs

Manipulation of data

Public figures

3rd party business partner access

Prevention of exploits

Scenarios

- “need to comply”
- GDPR, data privacy
- Export restriction/ITAR (also on data)
- Auditability
- Reporting (financial disclosure)

- Spin-offs: systems can’t be technically split in time
- Prevent inappropriate disclosure, data manipulation

- Data manipulation
- Example of salary changes
- Channel transactions to other accounts
- To damaged organization by creating data inconsistency: bind energy/create cost; create audit problems, damage reputation

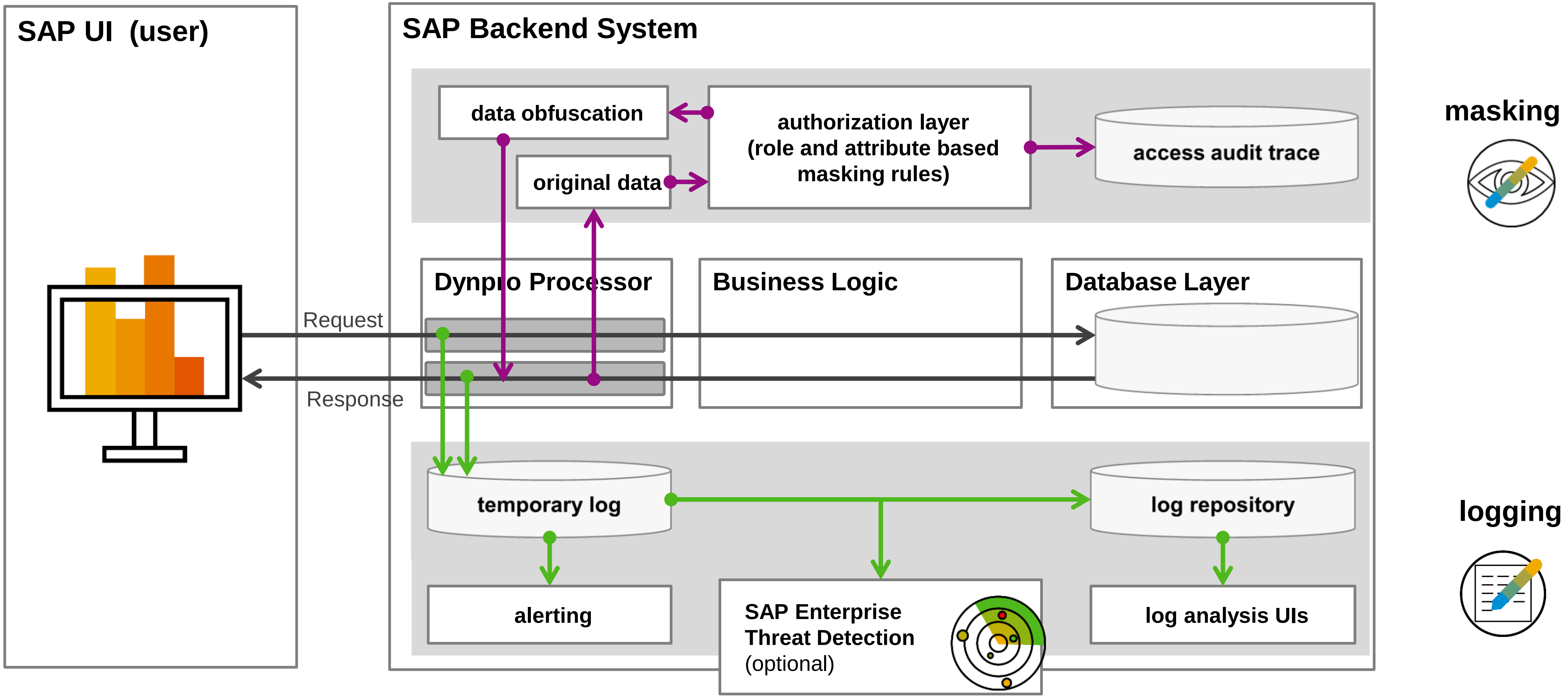
- “VIP scenario” – exposed persons
- E.g. “CEO” or sb’s management line
- “public figures”: public sector systems with hugely sensitive and unique private information, tax, dependents, criminal records…

- 3rd party users
- Call centre agents (external) for customer care or internal/IT
- Business partners, suppliers updating their master data, pricing, etc.

- Prevent exploits
- Segregation of duties scenario: actively prevent actions based on context e.g. magnitude
- Download of weak password hashes
- Attack intelligence on system setup, patch levels, protective mechanisms

UI Data Protection Masking & Logging

High level solution architecture



Key solution capabilities – UI Data Protection Masking

Key Capabilities of SAP UI Data Protection Masking

Concealing sensitive data on the UI layer in addition to existing authorizations

Sensitive data concealed at the field and object level
Data may be obfuscated in SAP UI fields partially or fully; or access to an object blocked completely

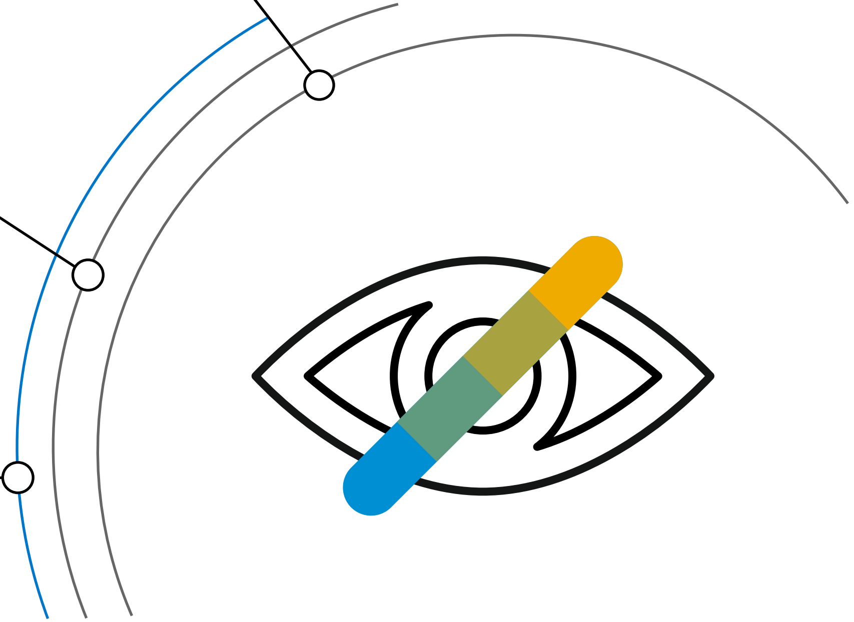
Field and object-level obfuscation

Access to sensitive data is attribute-based, ensuring that the right users get the right data at the right time

Attribute-based authorization

Flexibility for users to request sensitive information as required by their tasks

Reveal on-Demand



Key Features of UI Data Protection Masking for SAP S/4HANA

Configurable data protection in SAP UIs

- **Field level:** Masking field value, disabling the field on the UI; hiding fields on the UI; Clear fields on the UI and
- **disabling actions** (such as navigation and buttons)

"Data blocking" (GUI, UI5)

- Control navigation and actions; remove lines from tables

"Attribute based" access control

- **Rules** can be defined in the policy engine

Reveal On-Demand

- **Data initially always masked; a user action triggers authorization check and unmasking – action and result are documented.**

UI5/Fiori-based dashboard

- monitoring UI Data Protection Masking for SAP S/4HANA

UI5/Fiori-application-based configuration

- configuration menu is offered as a Fiori-based APP

UI Data Protection Masking used by Jabil Inc. https://www.jabil.com/

JABIL Turns to UI Masking for Stronger Data Protection Interview of Jabil's Cybersecurity Architect Wilder Latino, hosted by SAP Insider Senior Editor Fred Donovan https://www.sapinsideronline.com/videos/video-qa-jabil-turns-to-ui-masking-for-stronger-data-protection/

SAPinsider

To learn more about Jabil's UI data masking and other cybersecurity measures check out this video interview with Wilder Latino, SAP Cybersecurity Solutions Architect, Jabil.

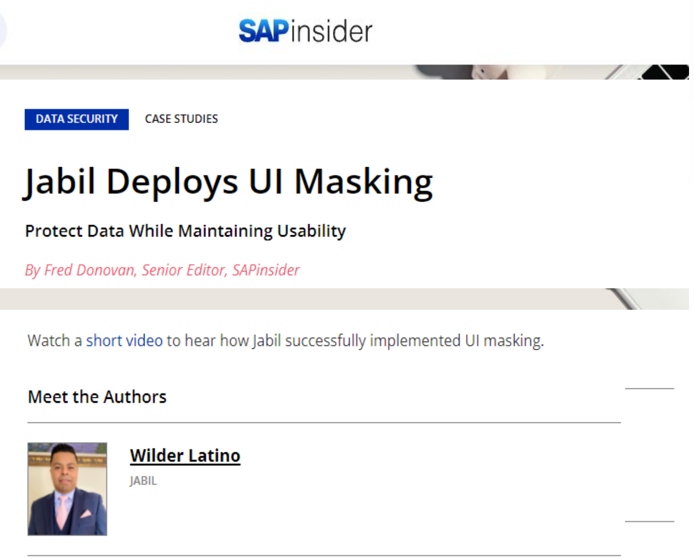
Watch:

SAP insider
Wilder Latino | SAP Cyber Security Solutions Architect, Jabil
Fred Donovan | Senior Editor, SAPinsider
03:02

Read the full story.

JABIL Deploys UI Masking – Article by SAP Insider Senior Editor Fred Donovan

https://www.sapinsideronline.com/case-studies/jabil-deploys-ui-masking-to-protect-data-while-maintaining-usability/


SAPinsider

DATA SECURITY CASE STUDIES

Jabil Deploys UI Masking

Protect Data While Maintaining Usability

By Fred Donovan, Senior Editor, SAPinsider

Watch a short video to hear how Jabil successfully implemented UI masking.

Meet the Authors

Wilder Latino
JABIL

Key solution capabilities – UI Data Protection Logging

Key Capabilities of SAP UI Data Protection Logging

Enabling UI level data access logging with real-time alerting and analysis tools

Audit trail of logs of user actions and data accessed in SAP UIs with sensitive content

Evidence for investigative purposes

Facility for data protection responsible roles to investigate events
Critical field identifiers for fast access and retrieval of relevant logs

Fast and user-friendly analysis

Alerts for critical data accesses
Complement to logs captured by SAP Enterprise Threat Detection for correlation

Near real-time alerts

Key Features of UI Data Protection Logging for SAP S/4HANA

Configurable logging scope in SAP UIs

- **Determine scope on application level** (GUI transaction, Fiori app…)

Versatile logging depths

- Complete logging (with filter options for data reduction)
- “Basic logging” for minimized data volumes
- Conditional logging determining whether, and how deep, access is logged.

Multiple DPO responsibilities

- multiple **data protection officers with different responsibilities** only get access to only the logs for which they’re responsible.

Data tagging for key and context

- Group key and critical context fields with identifiers
- allowing fast and user-friendly analysis of logged data

Alerting

- **Near-real time notifications** when certain data is accessed, through SAP notification framework
- Near real-time through integration with SAP Enterprise Threat Detection

DPO cockpit and log analyser

- Fiori based, streamlined analysis UI for business users
- Detailed log analysis tools for technical users

UIDP Masking demo

[life system demo]

UIDP Logging “slide” demo

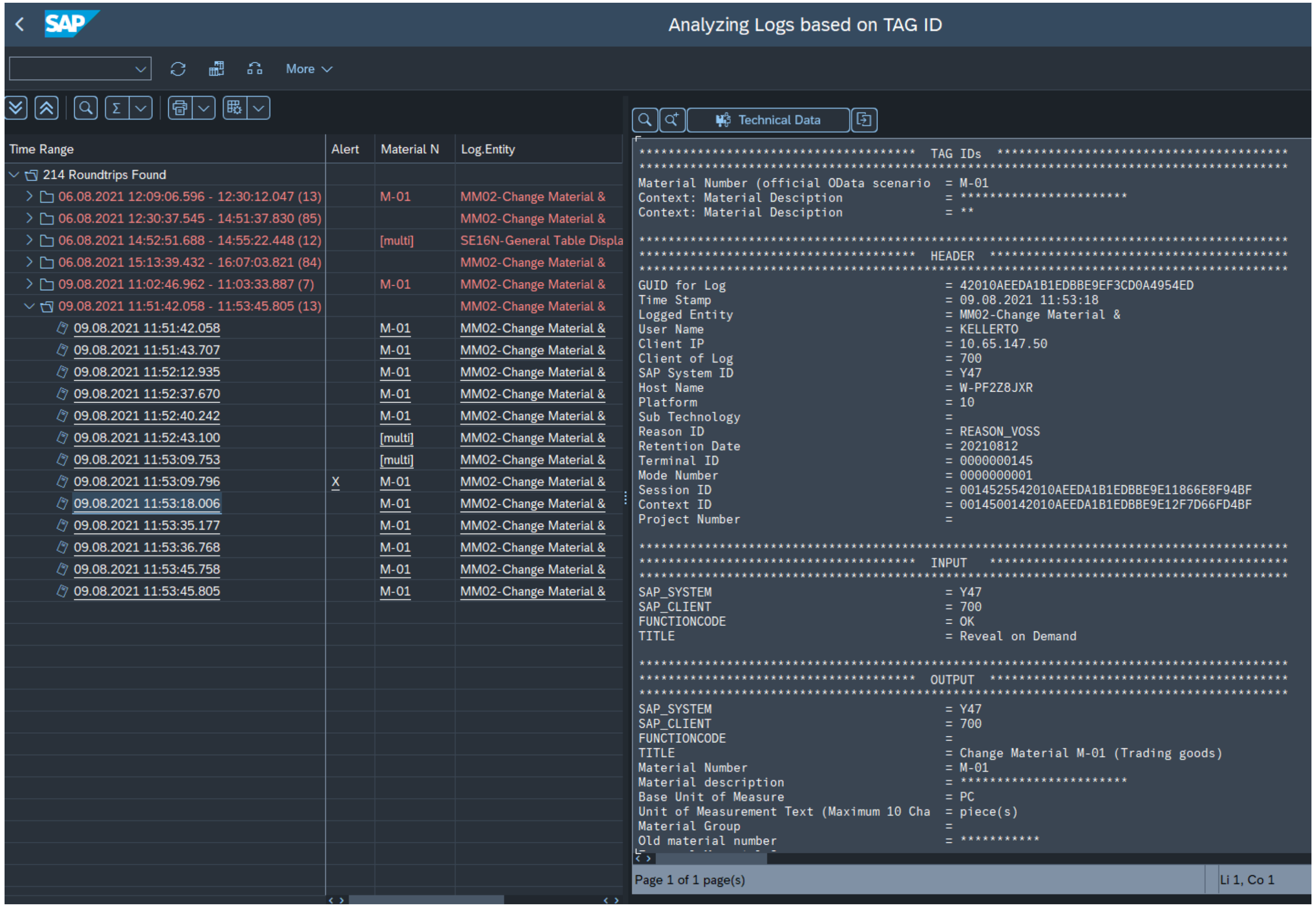
Data Protection Officer Analysis App

DPO Cockpit: Analysis of detailed access log (SAP GUI)

For a given selection, technical details can be displayed in a GUI transaction.

Per roundtrip (list on left side), the detail log information can be reviewed.

Besides Tags (highlighted), the log file includes header meta information identifying the context of the log (i.e. concerning the user), the explicit input, as well as the specific output.



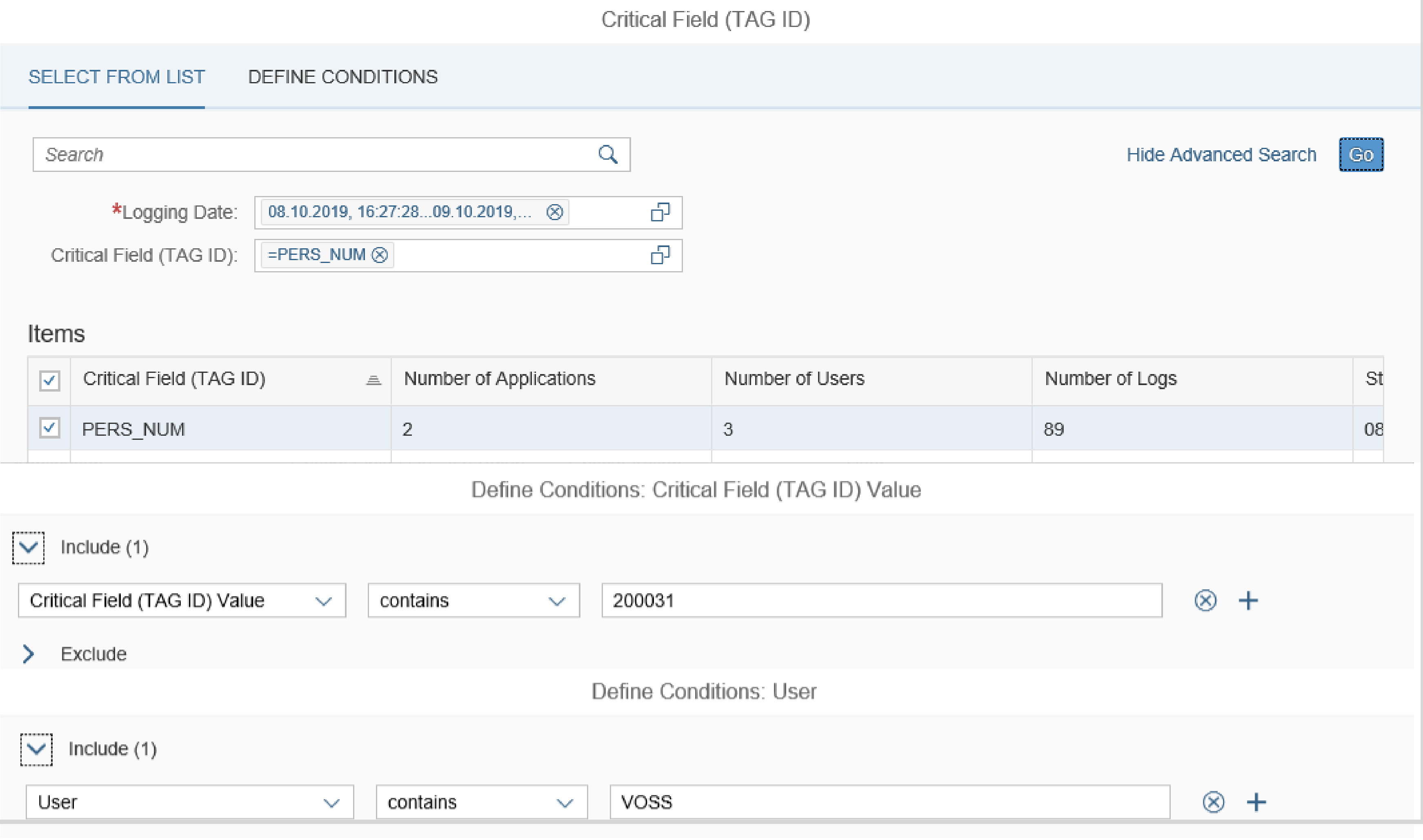
Time Range	Alert	Material N	Log.Entity
214 Roundtrips Found			
06.08.2021 12:09:06.596 - 12:30:12.047 (13)		M-01	MM02-Change Material &
06.08.2021 12:30:37.545 - 14:51:37.830 (85)			MM02-Change Material &
06.08.2021 14:52:51.688 - 14:55:22.448 (12)		[multi]	SE16N-General Table Displa
06.08.2021 15:13:39.432 - 16:07:03.821 (84)			MM02-Change Material &
09.08.2021 11:02:46.962 - 11:03:33.887 (7)		M-01	MM02-Change Material &
09.08.2021 11:51:42.058 - 11:53:45.805 (13)			MM02-Change Material &
09.08.2021 11:51:42.058		M-01	MM02-Change Material &
09.08.2021 11:51:43.707		M-01	MM02-Change Material &
09.08.2021 11:52:12.935		M-01	MM02-Change Material &
09.08.2021 11:52:37.670		M-01	MM02-Change Material &
09.08.2021 11:52:40.242		M-01	MM02-Change Material &
09.08.2021 11:52:43.100		[multi]	MM02-Change Material &
09.08.2021 11:53:09.753		[multi]	MM02-Change Material &
09.08.2021 11:53:09.796	X	M-01	MM02-Change Material &
09.08.2021 11:53:18.006		M-01	MM02-Change Material &
09.08.2021 11:53:35.177		M-01	MM02-Change Material &
09.08.2021 11:53:36.768		M-01	MM02-Change Material &
09.08.2021 11:53:45.758		M-01	MM02-Change Material &
09.08.2021 11:53:45.805		M-01	MM02-Change Material &

```
*************************************  TAG IDs  ****************************************
*****************************************************************************************
Material Number (official OData scenario  = M-01
Context: Material Desciption              = **********************
Context: Material Desciption              = **

*****************************************************************************************
*************************************  HEADER  *****************************************
*****************************************************************************************
GUID for Log                              = 42010AEEDA1B1EDBBE9EF3CD0A4954ED
Time Stamp                                = 09.08.2021 11:53:18
Logged Entity                             = MM02-Change Material &
User Name                                 = KELLERTO
Client IP                                 = 10.65.147.50
Client of Log                             = 700
SAP System ID                             = Y47
Host Name                                 = W-PF2Z8JXR
Platform                                  = 10
Sub Technology                            =
Reason ID                                 = REASON_VOSS
Retention Date                            = 20210812
Terminal ID                               = 0000000145
Mode Number                               = 0000000001
Session ID                                = 0014525542010AEEDA1B1EDBBE9E11866E8F94BF
Context ID                                = 0014500142010AEEDA1B1EDBBE9E12F7D66FD4BF
Project Number                            =

*****************************************************************************************
*************************************  INPUT   *****************************************
*****************************************************************************************
SAP_SYSTEM                                = Y47
SAP_CLIENT                                = 700
FUNCTIONCODE                              = OK
TITLE                                     = Reveal on Demand

*****************************************************************************************
*************************************  OUTPUT  *****************************************
*****************************************************************************************
SAP_SYSTEM                                = Y47
SAP_CLIENT                                = 700
FUNCTIONCODE                              =
TITLE                                     = Change Material M-01 (Trading goods)
Material Number                           = M-01
Material description                      = **********************
Base Unit of Measure                      = PC
Unit of Measurement Text (Maximum 10 Cha  = piece(s)
Material Group                            =
Old material number                       = ***********
```

Page 1 of 1 page(s)   Li 1, Co 1

DPO Cockpit: Analysis of UI Logs

Exploratory analysis of access to data types: comprehensive overview of data usage through field IDs (tags)
More granular display with additional filter criteria.



Critical Field (TAG ID)

*Logging Date: 08.10.2019, 16:27:28...09.10.2019,...

Critical Field (TAG ID): =PERS_NUM

Items

☑	Critical Field (TAG ID)	Number of Applications	Number of Users	Number of Logs	St
☑	PERS_NUM	2	3	89	08

Define Conditions: Critical Field (TAG ID) Value

Include (1)

Critical Field (TAG ID) Value | contains | 200031

Exclude

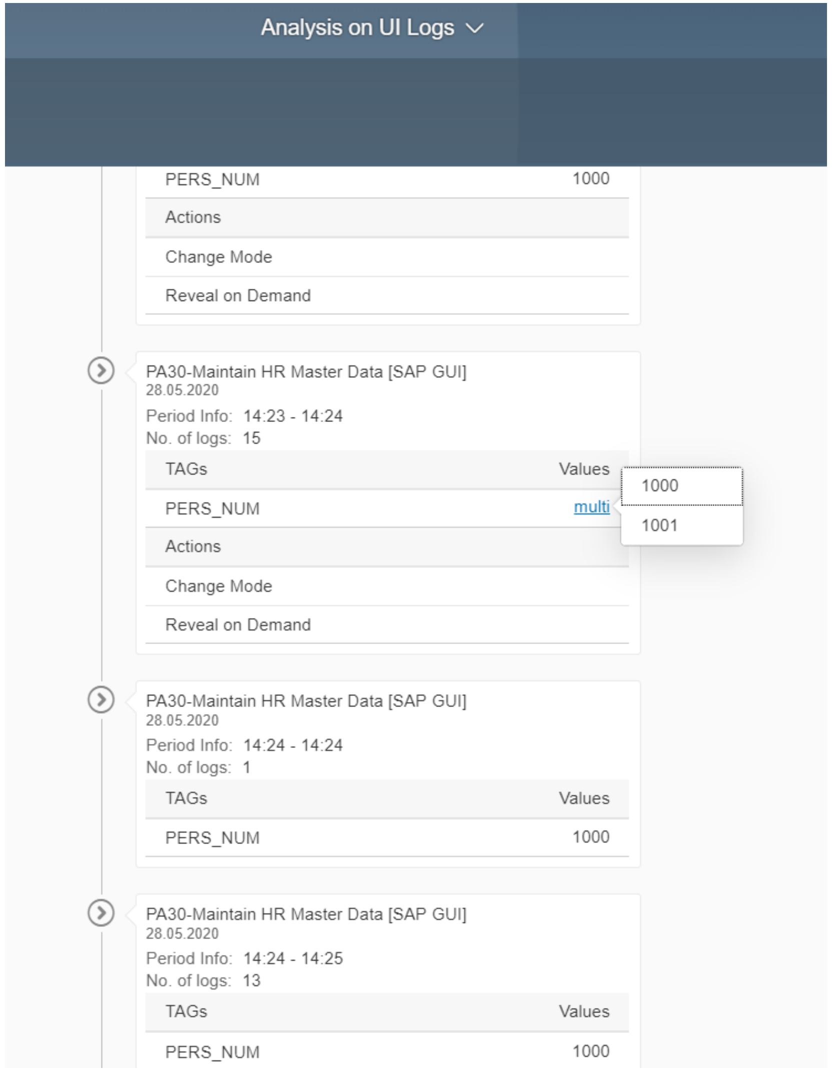
Define Conditions: User

Include (1)

User | contains | VOSS

DPO Cockpit: Analysis of User actions and their sequence

Sequential overview of a user's actions in aggregated view, indicating e.g. which critical/key fields were displayed, and of sensitive actions.



PERS_NUM	1000
Actions	
Change Mode	
Reveal on Demand	

PA30-Maintain HR Master Data [SAP GUI]
28.05.2020
Period Info: 14:23 - 14:24
No. of logs: 15

TAGs	Values
PERS_NUM	multi
Actions	
Change Mode	
Reveal on Demand	

1000
1001

PA30-Maintain HR Master Data [SAP GUI]
28.05.2020
Period Info: 14:24 - 14:24
No. of logs: 1

TAGs	Values
PERS_NUM	1000

PA30-Maintain HR Master Data [SAP GUI]
28.05.2020
Period Info: 14:24 - 14:25
No. of logs: 13

TAGs	Values
PERS_NUM	1000

Further Information

UIDP Masking and Logging | Roadmap Highlights

Key innovations

Version: 2022-03-16
SAP has 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's strategy and possible future developments, products, and platforms, directions, and functionality are all subject to change and may be changed by SAP 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.

UI Data Protection Masking and Logging

Recent/current activities

Recently completed (2021)

- Reveal on Demand integration with workflows
- Continuous improvements (PDF masking)
- Availability with S/4H and ECC Private Cloud Edition (RISE)

Ongoing activities (2022)

- Streamlined handling of mass log data
- Block access to GUI transactions and Fiori apps, based on ABAC policies
- Embedded analytics in SAP S/4H
- Support for additional languages in the application (French, Japanese, Spanish)

Planned activities (2023)

- BTP based UIDP solution with advanced data protection and analytical tools
- Extend data blocking via ABAC policies to
  - Web Dynpro ABAP
  - CRM Web Client UI
- Expand UI data protection coverage (e.g. SAC)
- Additional features of UIDP core – alerts, change logs, dashboards, data classification, etc.
- Data element (column based) encryption
- Data exploit prevention (authorization changes, config changes, brute force attacks, from SOD conflicts, etc.)

Future direction (2024+)

- Protection for Data Warehouse Cloud and BW4H
- data access prevention and transparency
  - coverage for native BTP apps
  - coverage for non-BTP cloud applications
  - advanced analysis tools
- Advanced data protection drawing on Multi Factor Authentication
- Machine Learning augmented data classification
- ABAC for Industry 4.0 (IoT)
- Dynamic consent

Thank you.

Tobias Keller
Product Manager UI Data Security
tobias.keller@sap.com

Deepak Gupta
Product Manager UI Data Security
deepak04.gupta@sap.com

Arun Verma
Product Owner UI Data Protection Masking
arun.verma01@sap.com

Further Information

SAP UI Data Protection Community Topic page:
https://community.sap.com/topics/ui-data-protection

→ Public presentation

→ UIML selected features – demo brief (7min)

→ UIML selected features & config options – demo long (ca. 28 min)

→ UI Masking overview & FAQ blog (product team)

Follow us

www.sap.com/contactsap

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.

THE BEST RUN SAP®