

SAP Solution Brief
SAP S/4HANA

Maximize Data Security with **UI Data Protection Masking and Logging**

THE BEST RUN



Data Security Matters **More Than Ever**

New legislation worldwide makes companies responsible for controlling who can access, view, and modify sensitive data internally and for tracking access, not just securing sensitive data. This requires a **flexible, granular way to limit access to critical fields to authorized key users** and track and analyze their access and actions – without modifying your SAP® software.

Data Security Matters More Than Ever

This is especially important for businesses running critical processes on enterprise software such as SAP S/4HANA®. For example, to comply with global regulations for personally identifiable information (PII) – as well as to protect sensitive corporate data such as customer information, prices, and bills of materials – you need a way to extend the standard role and authorization controls for your SAP software down to the field level inside particular user interface views. You also need a way to continuously track and analyze who is accessing critical data and when.

With the UI data protection masking and UI data protection logging packages for SAP S/4HANA, you gain all these capabilities and more. Together, they help you protect “crown jewel” data from internal and external threats by concealing data in the SAP software UI, supporting dynamic access determination and logging and analyzing access and actions so you can identify and respond to data misuse early – before it’s too late.

Protect Data with UI Data Protection Masking

The UI data protection masking package for SAP S/4HANA helps you comply with security, confidentiality, and data privacy requirements by masking sensitive values in SAP software UIs. A powerful add-on package, it enhances and technically integrates with UI data access channels offered for certain ERP systems from SAP, such as SAP S/4HANA. This is so you can restrict who gets to see critical information in transactions and applications without complex authorization setup, system modifications, or custom UIs and variants.

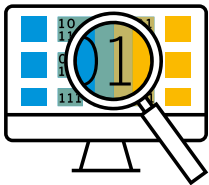
As an SAP S/4HANA customer, deploying our UI data protection masking package enables you to:

- **Define which data and screen fields to protect** and display in protected mode.
- **Take data protection actions** such as disabling or blocking complete data objects, restricting navigation, suppressing lines in tables, and restricting output options. These actions take place on the back-end server.
- **Specify who is authorized** to access data and under which circumstances.

Protect Data with UI Data Protection Masking

Detect and Respond Swiftly to Threats with UI Logging

Extend UI Masking and Logging Scenarios



IT staff, as well as data protection and security officers, can use the **built-in dashboard to monitor the software** in action.

- **Apply attribute-based authorizations** using metadata about the user and the data object, enabling dynamic determinations of data access authorizations based on context.
- **Activate reveal-on-demand controls** so that sensitive fields are initially masked independent of a user's authorization and are only unmasked after the user requests and justifies access, which is recorded for review and audit purposes.

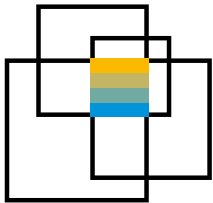
- **Define data security actions and authorizations at a data-element or table-field level** and have them consistently applied across sensitive mapped fields and supported UI channels.

UI data protection masking integrates with UI channels for ERP systems from SAP, including SAP GUI, SAPUI5, the SAP Fiori® user experience, the field masking for Web Client UI solution (for CRM), and the Web Dynpro development environment for ABAP.

Protect Data with UI Data Protection Masking

Detect and Respond Swiftly to Threats with UI Logging

Extend UI Masking and Logging Scenarios



UI masking authorizations can be configured on top of an existing authorization setup for a role, or they can be **integrated with existing business roles.**

Detect and Respond Swiftly to Threats with UI Logging

Compliance with data protection regulations also requires tracking and reporting on who has access to sensitive data captured and held by your organization – and who attempted to access sensitive, protected information. This data also helps you identify potential data abuse and abusers.

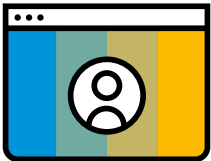
The UI data protection logging package for SAP S/4HANA supports comprehensive, consistent logging of data access based on configurations

you define. Logging, combined with analytics and visibility into who has accessed or viewed what data, enables you to detect issues early – and even in near-real time – and respond swiftly to minimize the severity of data exposure. You'll not only facilitate compliance with your internal and legal data security requirements for sensitive data but also reduce the financial and reputational risk from data theft and abuse.

Protect Data with UI Data Protection Masking

Detect and Respond Swiftly to Threats with UI Logging

Extend UI Masking and Logging Scenarios



Gain deep and wide logging information about user activity with **minimal time and effort**.

As an SAP S/4HANA customer, deploying UI data protection logging enables you to:

- **Implement UI-based logging functions** that record data displayed to and entered by users.
- **Reduce log volumes** by filtering and storing the most relevant data.
- **Manage logged users** based on users, roles, profiles, and groups using an allow-list or block-list approach.

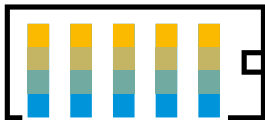
- **Set up real-time alerting** so that security officers receive notifications when specified data is accessed.
- **Assign tags to key fields and other relevant content.** Tags make logging data searchable, retrievable, and easier to analyze and audit.

UI data protection logging integrates with UI channels for ERP systems from SAP, including SAP GUI, SAPUI5, SAP Fiori, the logging of Web Client UI solution, Web Dynpro for ABAP, the logging of SAP BW access solution, Remote Function Call (RFC), and Web services.

Protect Data with UI Data Protection Masking

Detect and Respond Swiftly to Threats with UI Logging

Extend UI Masking and Logging Scenarios



Minimize data storage with condensed logging and conditional logging so you **retain only the data you need for analysis.**

Extend UI Masking and Logging Scenarios

UI masking and logging packages are also available for SAP ERP Central Component (SAP ECC) scenarios. They offer the core features and capabilities noted for the same UI technologies as for SAP S/4HANA.

In addition, you can also integrate UI logging with the SAP Enterprise Threat Detection application to set up the transfer of logged data to this application. Integration is smooth, and you can automate the analyses of log files. Correlating logs in real

time enables you to uncover statistical outliers and dubious patterns of user behavior that may indicate risk. As a result, you can identify and respond to data threats before serious damage occurs.

When you integrate both masking and logging packages with SAP Enterprise Threat Detection, the software can be built to automatically react to potential threats in real time. For example, it can dynamically restrict actions a user can perform and mask data previously accessible to them.

Protect Data with UI Data Protection Masking

Detect and Respond Swiftly to Threats with UI Logging

Extend UI Masking and Logging Scenarios



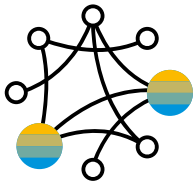
UI masking and logging packages work as stand-alone solutions – but when deployed together, they help provide even more ways to **protect your valuable data**.

Realize the Benefits

Now there's an easier to use, configurable, and dynamic way of controlling data access and visibility within SAP S/4HANA, as well as capturing and analyzing logging data to detect and address data abuse early. You can protect sensitive business information by restricting access to a small, approved audience – reducing your risk from “insiders” abusing or leaking data by restricting access to it. You can also facilitate compliance with data security and privacy laws and business requirements.

With continuous logging of access across the enterprise, you reap the benefits of data access transparency and actionable information and alerts. For example, your people become more aware of their responsibility toward sensitive data and tend to minimize casual, careless, and other non-task-related attempts to access it. And in cases of data misuse, you can act quickly to potential threats and reduce the severity of data misuse cases.

Realize the Benefits



Use UI data protection masking and logging packages to **enhance capabilities of SAP Enterprise Threat Detection** and other automated security and incident-monitoring solutions.

Summary

The UI data protection masking and logging packages from SAP increase data security in supported UIs without the need for software modifications. With the UI data protection masking package for SAP S/4HANA®, you can configure granular, contextual authorizations for access to sensitive data that are applied to data security actions on the UI layer at runtime. The UI data protection logging package for SAP S/4HANA tracks data access attempts, providing visibility and alerts as needed to reduce risk from data theft and abuse.

Objectives

- Facilitate compliance with legal requirements for data protection
- Limit risk of falling victim to data being stolen, abused, or leaked
- Enable masking and logging down to the field level without modifying SAP® software

Solution

- Protect sensitive data from insiders by restricting navigation to data, blocking it from view, limiting actions, and configuring dynamic access permissions based on context
- Track and log data access requests and successes for sensitive data, and use this data to detect threats early, take action, and report to authorities
- Manage data volumes using policy engine determinations

Benefits

- Continuous compliance with internal and external data security and privacy requirements
- Faster, earlier detection and mitigation of data breaches and abuses
- Protection of your brand

Learn more

To find out more, call your SAP representative today or visit us [online](#).



Follow us



www.sap.com/contactsap

Studio SAP | 72713enUS (21/02)

© 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/trademark for additional trademark information and notices.

THE BEST RUN 