

2016-09-27

# Release Notes for SAP Access Control for S/4HANA



---

# Content

**1**    **Release Notes for SAP Access Control for S/4HANA..... 3**

# 1 Release Notes for SAP Access Control for S/4HANA

## Technical Data

Table 1:

<b>Product Version</b>	10.1
<b>Area</b>	SAP Access Control
<b>Country Relevance</b>	Valid for all countries

Key features:

- **Ability to run exclusively on SAP S/4HANA** – SAP Access Control, Process Control and Risk Management 10.1 on S/4HANA run on SAP S/4HANA.
- **Simplified Access Request** - SAP Access Control 10.1 features a new, simplified, and intuitive Access Request form allowing you to define Request Reasons and to use these reasons for request selection. You can click the role name and access critical information such as Tcodes and you can save a draft version of the request. You can also add comments for each role. New side panels provide additional information such as the details of risk analysis.
- **Custom User Groups from SU01 Attributes** - You can now create custom user groups based on SU01 attributes. You can use these groups when performing risk analysis.
- **System-Specific Org Rule Analysis** - You can now define and activate the Org Rules for specific systems only. Using organizational rules in risk analysis can be time consuming especially in batch risk analysis. In most cases, Org Rules only apply to some of the connected ERP systems. By having system-specific Org Rules, only the relevant rules are used for risk analysis resulting in highly improved run times.
- **Org Rule Maintenance Wizard** - The Org Rule Maintenance Wizard makes creating organizational rules faster, easier and eliminates possible invalid entries due to manual input errors. The wizard allows you to select the desired ERP system, select the Rule Sets, select the Organizational Levels from existing risks, and select Organizational Level values from the ERP system. You can then review and edit the new rule before generating it.
- **Context-Based Side Panels** - This new user interface feature, an alternative to the dialog box, provides more on screen information about the process you are using without requiring you to leave the main screen. For example, while working on the access risk screen, you can use the Violation Historic View side panel to display the number of users associated with this access risk over time and also the number of mitigations over time.
- **Access Control for SAP HANA** - This feature enables SAP Access Control to manage access and risk analysis for SAP HANA based authorizations to support SAP HANA Performance Applications and SAP HANA Business Analytics.
- **Role Search Personalization** - You can now add custom fields to the role search criteria for access requests and configure the field attributes to the following values: **Display** only, **Hidden**, or **Default**.
- **Context Sensitive Help** - You can directly access the help topics for the process you are executing by clicking on the application screen and accessing the Help Center.

---

## Enhanced Features

- **Improvements to Access Risk Analysis and Remediation**
  - **Access Risk Root Cause Analysis** - The access risk root cause analysis remediation view enables easier identification and remediation of access risks. It offers a set of tools for segmenting risk violations so you know which risks to target first. You can enable remediation workflow processes from the remediation view to ensure that the processing and auditing of remediation activities are followed and tracked.
  - **Extended Remediation Capabilities** - Remediation capabilities are extended by allowing reviewers to initiate removing roles or editing role validity dates directly from the access risk analysis results. These two new workflow processes are fully configurable and may reuse routing and approval rules from any other GRC workflow process. This functionality is available for both SAP Access Control and the integrated access risk analysis portion of SAP Process Control.
- **Reporting & Dashboard Authorization** - Reports and dashboards are now secured using role-based authorizations. In addition, users' authorizations can be displayed in a dialog box when desired. An administrator can enable or disable this link for display.

## More Information

For more information, see the application help **SAP Access Control** at <https://help.sap.com/grc-ac>.

---

# Important Disclaimers and Legal Information

## Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

## Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

## Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

## Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>).





**go.sap.com/registration/  
contact.html**

© 2016 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.  
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.  
Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.