OpenText™ Axcelerate 5.13.1 (On Premise)

Custom User Security Options

Published: 2017-Dec-01

Contents

1 Custom Security Options for Axcelerate 5 3
1.1 How Apply Custom Security to Documents Works 4
1.2 Apply Custom Security to Documents Use Cases 5
1.3 Apply Custom Security to Documents Limitations 6
2 Contact Us 7
3 Terms of Use 8

1 Custom Security Options for Axcelerate 5

In addition to preconfigured user roles, Axcelerate 5 provides a range of custom security options. Some of these options can be set by Case Managers; most are set by Administrators.

The available custom security options for Axcelerate 5 are:

Arrangement Security

Users with an All or Case Manager user role can restrict user groups from seeing specific arrangements on the **Analysis** and **Review** pages.

Note: If an All user restricts a Case Manager user group, the Case Manager group cannot manage the restricted arrangement(s) on the **Administration > Arrangements** page.

Field Security

Users with an All or Case Manager user role can make fields read-only on an arrangement-level. The Case Manager must have access rights to the arrangement.

Add To or Remove Axcelerate 5 User Role-Based Rights

An Administrator can add to or remove some of the Axcelerate 5 preconfigured user role rights for user groups. This includes:

- Download native files
- Viewer feature rights, used in conjunction with the **Apply Custom Security to Document** field:
  - Download of restricted documents
  - NEAR NATIVE view for restricted documents
  - IMAGE view for restricted documents
  - REDACTION view for restricted documents
- Manage batches
- Bulk tag documents
- View associated documents outside of batch
- Manage rights of users to pull batches
- Add and modify field values on the **Tagging** and **Foldering** panels
- Manage fields via the **Fields and Values** page
- Manage arrangements

- Access document history
- Manage batching templates

Consult with your Administrator if this type of security is available and desired in your Axcelerate 5 matter.

1.1 How Apply Custom Security to Documents Works

The **Apply Custom Security to Document** field was added with the Axcelerate 5.13.1 release. It is a multi-value tagging field that is used in conjunction with application-level security to restrict user groups from downloading native files and/or accessing certain document views for restricted documents.

To apply and use this security:

1. The Case Manager and Administrator mutually agree on the restrictions and to which users they shall apply.
2. The Administrator creates user group(s) with the appropriate application-level security configuration, e.g., download of restricted documents is not allowed.
3. The Case Manager adds the **Apply Custom Security to Document** field to a tagging arrangement.
4. Users that are allowed to see all documents begin their review. When they identify a document with privileged content that should not be fully accessible to other users, they tag the appropriate value(s) in the **Apply Custom Security to Document** field, i.e., **Restrict Download**, **Restrict Image view**, **Restrict Near Native view**, and/or **Restrict Redaction view**.

Once the restrictions are in place, users that are part of the restricted user group(s) can access Axcelerate 5. When they come across a restricted document, they do not see the respective feature, e.g., the **Download** button.

Note: The restriction applied to a document is only effective when the application-level security applied to a user group matches the restriction.

Example

User Group One Security

Cannot download restricted documents.

User Group Two Security

Cannot access **Near Native** view for restricted documents.

Document Restriction

A document is tagged **Restrict Download** and **Restrict Redaction View**.

Result: Group One cannot download the document, but can still access **Redaction** view. Group Two can download the document and can also use **Redaction** view. Unless a group is restricted from **Redaction** view, the **Restrict Redaction View** tag has no restrictive power.

1.2 Apply Custom Security to Documents Use Cases

You may want to disallow certain viewer features for specific users, like native download or viewing the **Near Native** or **Redaction** view. You can do so for all documents or for only certain documents. For example:

Hide features to improve review speed

You do not want reviewers to click the **Near Native** view because this starts conversion and the reviewers do not need this view.
In this case, an Administrator would add all reviewers to a user group that is not allowed to access **Near Native** view. Additionally, someone on the project team would tag the **Restrict Near Native view** value of the **Apply Custom Security to Document** field for all documents in the Axcelerate 5 project.

Forbid redactions for a certain reviewer group

You do not want certain reviewers to apply redactions, so you hide the **Redaction** view from this user group.
In this case, an Administrator would add the identified reviewers to a user group that is not allowed to access **Redaction** view. Additionally, someone on the project team would tag the **Restrict Redaction view** value of the **Apply Custom Security to Document** field for all documents in the Axcelerate 5 project.

Hide privileged content from certain users

In Axcelerate 5, some content related to privileged attachments or embeddings may still be viewable by users, even though an Administrator has applied document level security. The reason is that when conversion accesses the parent document, it also converts content or other information

related to any attachments or embeddings. In **Near Native** view, users may, for instance, see a converted Microsoft Word document that contains a link to a privileged embedded Excel sheet. Or if they download an email, this will reveal all attachments and embeddings, even privileged ones.
In this case, an Administrator would add the identified users to a user group that is not allowed to download restricted documents, nor access the **Image** view, **Near Native** view or **Redaction** view of the restricted documents. Additionally, someone on the project team would tag all of the values of the **Apply Custom Security to Document** field for all applicable documents in the Axcelerate 5 project, i.e., **Restrict Download**, **Restrict Image view**, **Restrict Near Native view**, and **Restrict Redaction view**.

1.3 Apply Custom Security to Documents Limitations

No security for Text view

Text view cannot be restricted.

Deleting values of the Apply Custom Security to Document field makes security related to this value impossible

If a user deletes any of the **Apply Custom Security to Document** field values, those values can never be restored to their original functionality.

Modifying Apply Custom Security to Document field values is only possible in the Axcelerate 5 front end

Renaming a field value in CORE Administration can affect the value's functionality as the values are linked to security configuration.
Renaming a field value in Axcelerate 5 does not affect the functionality, . If you rename a value, make sure that users still understand the restriction.

Access to Viewer Functionality

Application-level Security is not designed to deny access to functionality but rather to allow functionality for user groups. If users are members of groups that are allowed access to partially privileged documents, those users will always be allowed to see the entire document.

2 Contact Us

About Recommind

Recommind provides the most accurate and automated enterprise search, automatic classification, and eDiscovery software available, giving organizations and their users the information they need when they need it.

Visit us at **http://www.recommind.com**.

Support

For support issues on Recommind products, visit the Recommind Ticketing System at **https://rts.recommind.com**.

Documentation

Find Recommind product documentation, Knowledge Base articles, and more information at the Recommind Customer Portal at **https://supportkb.recommind.com**. For login access to the site, contact your product support:

- For : **SearchSupport@recommind.com**
- For : **Axcelerate@recommind.com**

The Recommind Documentation team is interested in your feedback.

For comments or questions about Recommind product documentation, contact us at **rec-documentation@opentext.com**.

3 Terms of Use

Disclaimer

This document, as well as the products and services described in it, is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Recommind, Inc., including its affiliates and subsidiaries (collectively, "Recommind"). Recommind assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software or services that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Recommind. Information in this document is provided in connection with Recommind's products and services. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document.

EXCEPT AS PROVIDED IN RECOMMIND'S SOFTWARE LICENSE AGREEMENT OR SERVICES AGREEMENT FOR SUCH PRODUCTS OR SERVICES, RECOMMIND ASSUMES NO LIABILITY WHATSOEVER, AND RECOMMIND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF RECOMMIND PRODUCTS OR SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. RECOMMIND MAKES NO WARRANTIES REGARDING THE COMPLETENESS OR ACCURACY OF ANY INFORMATION, NOR THAT THE PRODUCTS OR SERVICES WILL BE ERROR FREE, UNINTERRUPTED, OR SECURE. IN NO EVENT WILL RECOMMIND, THEIR DIRECTORS, EMPLOYEES, SHAREHOLDERS AND LICENSORS, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS OR BENEFITS.

Recommind may make changes to specifications, and product and service descriptions at any time, without prior notice. Recommind's products may contain design defects or errors known as errata that may cause the product or service to deviate from published specifications. Current characterized errata are available on request. Whilst every effort has been made to ensure that the information and content within this document is accurate, up-to-date and reliable, Recommind cannot be held responsible for inaccuracies or errors. Recommind software, services and documentation have been developed and prepared with the appropriate degree of skill, expertise and care. While every effort has been made to ensure that this documentation contains the most up-to-date and accurate information available, Recommind accepts no responsibility for any damage that

may be claimed by any user whatsoever for the specifications, errors or omissions in the use of the products, services and documentation.

Trademarks and Patents

Recommind's underlying technology is patented under *U.S. Patent Nos. 6,687,696, 7,328,216, 7,657,522, 7,747,631, 7,933,859, 8,024,333, 8,103,678, 8,429,159 and 8,489,538*

Recommind, Inc. is the leader in predictive information management and analysis software, delivering business applications that transform the way enterprises, government entities and law firms conduct eDiscovery, enterprise search, and information governance. The Recommind, Axcelerate, Axcelerate Cloud, Axcelerate OnDemand, CORE, Decisiv, Predictiv, MindServer, Auto-File, Smart Filtering, Insite Legal Hold, QwikFind, Perceptiv Contract Analysis, and EasyExport name and logo are trademarks or registered trademarks of Recommind, Inc. or Open Text.

Copyright