OpenText™ Axcelerate 5

Security for CORE Administration

Published: 2017-Aug-07

Contents

1 About this Document

This document describes security in CORE Administration with new security features added to the product after release. They are included in these software versions:

- CORE_5.17_840 for Axcelerate 5.11
- CORE_5.18_749 for Axcelerate 5.12

To check your software version, log in to CORE Administration and hover over the CORE Administration logo.

2 User Security for CORE Administration

User accounts must be created for the staff who will work in CORE Administration. There are different user roles to choose from, as well as custom security options to consider.

2.1 Security for CORE Administration Limitations

Default admin user

If you split Administrators in superusers and non-superusers and the default **admin** user is one of the non-superusers, he gets more rights than other non-superusers: this user can still see and access all workspaces and applications. Within the workspaces and applications he has the same restrictions as other non-superusers.
To return the default **admin** user to full power, add the **admin** user to the **List of superusers**

No file access restrictions for backend processes

Backend processes still operate on same resources. For example, logs will contain information from multiple workspaces.

File access restrictions are not applied to command lines

Users with command line access can access all files via a command line.
To avoid access from CORE Administration, you can forbid creation of command line tasks and reports for all users, e.g., in the **Task Scheduler** or for reports. All users can, however, still run command lines in the backend.

Tip: To prevent command lines from being run outside of CORE Administration, make sure users with direct access to the operating system do not have access to command line tools.

Related:

"Forbid creation of command-line tasks" on page 17

"Forbid creation of command-line reports" on page 18

2.2 User Roles for CORE Administration

The chart below lists the CORE Administration user roles and explains the differences between the roles.

Administrator (superuser)

Has access to all functions in CORE Administration in all workspaces and in all applications. In a newly installed system, all Administrators are superusers by default.

Administrator (non-superuser)

You do not see *non-superuser* in any roles list. Non-superuser Administrators only exist if at least one superuser Administrator is defined for CORE Administration.

Tip: To determine whether you are a superuser, go to the **Monitoring** tab. You are a superuser if you see the **Alerts** tab.

These users do not have access to functions that may show data beyond their allowed workspaces.

Specifically, these functions are excluded for non-superusers:

- Grant user access to applications

  They do not see the **Security** panel. They can only set roles for specific applications on the **Applications** panel (not on the **Computers** panel).
- On the **Computers** panel:
  - Define and assign pools for hosts on the **Roles** and **Pools** tabs
  - Define paths for projects on servers on the **Locations** tab
  - **Manage Hosts** for the Workspace
  - Tomcat configuration
  - Stop, start or remove Tomcat
  - Define aliases for Tomcat
- Monitoring tab:
  - Information outside accessible workspaces
  - **Alerts** tab
  - **Hardware** tab
- Create workspaces

Other non-superuser roles

All roles that are not Administrators are always non-superuser roles.

Configuration

These users do not have access to functions that may show data beyond their allowed workspaces. They do have access to all functions allowed for the **Operator** role, plus:

- Configuration of applications, engines, document models, data sources
- Add computer (workspace)
- Create application
- Export (application)
- Create Workspace
- Create application
- Create Data Source
- Create document model (Decisiv Search only)
- Add engine
- Merge CSV
- Print stack traces
- Add application (Decisiv Search only)
- Reload index configuration
- Drop template
- Set template
- Import (application)
- Clone field
- Remove

Operator

These users do not have access to functions that may show data beyond their allowed workspaces. They do have access to these functions:

- Start
- Stop
- Restart
- Kill
- Suspend (data source)
- Resume (data source)
- Wake

- Update computer statistics (client agent)
- Enable/disable (client agent)
- Apply write lock/write unlock (index engien)
- Save (engine)
- Enable/disable autostart
- Set active/inactive (application)
- Ensure all engines running (Axcelerate Ingestion)
- Delete Storage (data source)
- Clear project
- Export (engine)
- Change index location (index engine)

Monitoring

This is the weakest role.

These users do not have access to functions that may show data beyond their allowed workspaces. They only have access to these functions:

- Access to **Monitoring** tab
- See status of an application's components
- View log files

Related:

"Best Practices for Application Creation" on page 23

"Hide empty workspaces" on page 18

2.3 Assign Roles for CORE Administration

Required: In CORE Administration, there are users that can be assigned administrative roles.

1. In CORE Administration, open the **Default** workspace.

   If the **admin** application is in another workspace, open this one.
2. Select the **admin** application and, from the **Actions** menu, select **Grant access**.

   The **Assign application** window displays.
3. Set the desired group or user to **Allowed** in the **Access** column.

4. Click **OK**.
5. Keep the application selected and, from the **Actions** menu, select **Configure roles**.
6. For each user or group select the desired role in the **Roles** column.

   Tip: Although you see combinations of roles when you configure roles, it is sufficient to select one role, as the Administrator role contains Configuration, Operator and Monitoring roles, the Configuration role contains the Operator and Monitoring role, and the Operator role contains the Monitoring role.

7. Click **OK**.

2.4 The Default Admin User

After a default installation, there is exactly one user who has access to all workspaces and functions in CORE Administration, although he is not shown as user in the **Security** tab settings: the **admin** user.

The **admin** user also has access to back end scripts and applications.

So he has more rights than any user that you create in CORE Administration and that you assign the Administrator role.

Depending on company security policies, you may want to keep this **admin** user, restrict his rights or not allow this user at all.

You want to keep the admin user

If you specify any superuser for CORE Administration, specify the **admin** user, too. If you specify other users, but not the **admin** user, he can still access all workspaces but will be restricted to non-superuser for all other CORE Administration functionality.

If you don't specify any superuser, no action is needed.

You do not want to use the admin user

First create at least one Administrator in CORE Administration. If you want to split Administrators in superusers and non-superusers, add at least one Administrator to the superusers.

Then change the **admin** user's password, and do not forward it to anybody. Ask Recommind Support for details.

Also, replace the **admin** user in all back end utilities with an appropriate system administrator. Ask Recommind Support for details.

2.5 Split Administrators into Superusers and Non-superusers

In a newly installed system, all users with an Administrator user role are superusers. To make some Administrators non-superusers, you explicitly specify which Administrators should keep the superuser property. All other Administrators then become non-superusers.

Important: We recommend to specify the default user admin as superuser. The admin user has special rights outside CORE Administration that no other Administrator has by default.

To do so:

1. In CORE Administration, open the **default** workspace and select the **Applications** panel.
2. Open the configuration of the **admin** application in internal mode.

   Tip: To open an item's configuration in internal mode, select it, hold [SHIFT] and click .
3. Go to the **Cross workspace administration** node.
4. Enter your user name to the **List of superusers**, or add your user group's name to the **List of supergroups**.

   Add other users as appropriate.

   Tip: If you want the default **admin** user to retain full power, be sure to add that user to the **List of superusers**.
5. Restart the **admin** application.

Result: All Administrator users or groups that do not appear in the lists are now non-superusers.

Related:

"Administrator (non-superuser)" on page 5

2.6 Access to Workspaces

By default, access to workspaces is restricted for all non-superusers, i.e.:

- Users with the Configuration role
- Users with the Operator role
- Users with the Monitoring role

They are allowed to

- Access all empty workspaces

  Tip: If you do not want these users to get access to empty workspaces, activate the **Hide empty workspaces** option for the **admin** application.

- Access non-empty workspaces if they are granted access to at least one application in the workspace.

  This is also valid for the **Default** workspace.

  Note: Access to administrative applications is ignored. Administrative applications are, e.g., **admin** (CORE Administration), **cm** (Case Management Tool), **ls** (Log File Viewer), **searchWebApi** and **am** (Application Manager). So, if a workspace only contains administrative applications, these users will not see this workspace, even if they are granted rights to these applications.

If at least one superuser is specified

Access to workspaces is restricted in the same way as above, but this time, non-superusers also include

- Non-superuser Administrators

2.7 Restrict Access to CORE Features

You must have one of the following user roles to conduct these tasks:

- CORE Administrator (superuser)
- Configuration or Administrator (non-superuser), but only if you have access to the workspace containing the **admin** application.

You can restrict the access to the following CORE Administration and Axcelerate Ingestion features for all users, including superusers:

- Access to the **Explore** tab in CORE Administration

  You can disallow access to the **Explore** tab if administrative staff are not allowed to see documents.

- Creation of command line tasks

  Disallow if there is a risk that inexperienced users may cause exceptions with a command line task.

  Tip: For creating a single task, allow this feature, create the task and then disallow the feature again.

- Creation of command line reports
- Configuration of items in internal mode

  Note: Once enabled, this setting cannot be undone without assistance from Recommind Support.

You can also restrict all non-superusers from accessing the following features:

- Access to empty workspaces
- Access to the **Hardware** tab on the **Monitoring** tab in CORE Administration
- Access to the **Hardware** tab on the **Monitoring** tab in the Axcelerate Ingestion module (As the superuser roles does not exist for Axcelerate Ingestion, even users that are superusers in CORE Administration will not see this tab.)

Restrict access to these features in the **admin** application that you usually find in the **Default** workspace. Settings are part of the **Visibility** node, which is only shown in internal mode.

Tip: To open an item's configuration in internal mode, select it, hold [SHIFT] and click .

Related:

"Hide Explore Tab" on page 17

"Forbid creation of command-line tasks" on page 17

"Forbid creation of command-line reports" on page 18

"Allow internal settings with 'SHIFT'+configure" on page 18

"Hide empty workspaces" on page 18

"Hide Hardware tab (Administration)" on page 19

"Hide Hardware tab (ECA/Ingestion)" on page 19

2.8 Restrict File Access

You must have one of the following user roles to conduct these tasks:

- CORE Administrator (superuser)
- Configuration or Administrator (non-superuser), but only if you have access to the workspace containing the **admin** application.

You can specify the file system folders that non-superusers have access to when working in CORE Administration or in the Axcelerate Ingestion module.

Note: In the Axcelerate Ingestion module, all users are treated as non-superusers, even those that are superusers in CORE Administration.

How does file access work?

When a non-superuser logs in or switches workspaces, the configuration of the **admin** application in the default workspace of CORE Administration is checked.

If file access for the specific workspace is defined, only this file access is allowed.

If no file access for the specific workspace is defined, file access for multiple workspaces applies, provided it matches existing filepaths.

If the file access defined for multiple workspaces does not match existing filepaths, the non-superuser has access to the complete file system.

Caution: Never grant a non-superuser access to a custom application in the workspace that contains the **admin** application. If you do, the user may change the settings described here.

Required:

- Workspaces and file system folders use a naming scheme that allows for the use of regular expressions.

To restrict file access for non-superusers:

1. In CORE Administration, open the **Default** workspace and select the **Applications** panel.
2. Open the configuration of the **admin** application in internal mode.

   Tip: To open an item's configuration in internal mode, select it, hold [SHIFT] and click  .

3. Go to the **Cross workspace administration** node.

4. In the **Regex to limit file access** field, define file access with regular expressions for multiple workspaces.

   If you use the placeholder CLIENTID_FROM_WORKSPACEID, you can specify a pattern for character extraction from the workspace ID.

5. For a workspace where the file access defined in the **Regex to limit file access** field does not work, but that non-superusers must have access to, use the **Non-superuser file access in individual workspaces** area to map this specific workspace to a regular expression for file access.

6. Click **OK** to save.

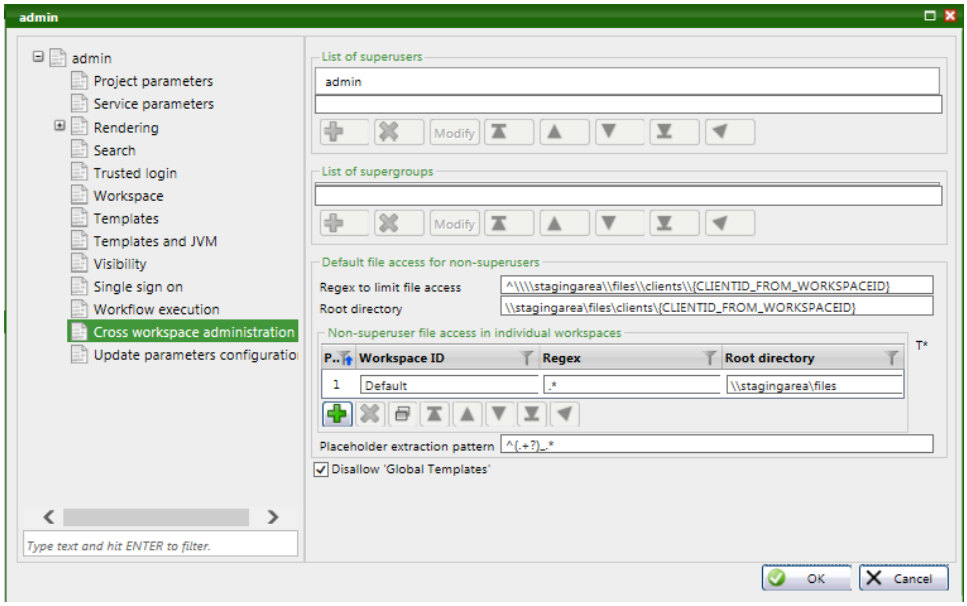
Result: The configuration is automatically applied when a user changes workspaces or logs in to the Axcelerate Ingestion module. A restart of the application is not required for this access configuration.

Note: Invalid regular expressions will not open any folders for a workspace. Errors are logged as [E2] Invalid file restriction .....in the CORE Administration log file.

What happens if an application existed before and feature configuration, e.g., for storages, contains paths not matching the regular expression?

Everything works like before. All paths configured previously can be used. But if a non-superuser tries to change a path in the project configuration, he can only change it to a path matching the regular expression.

Cross workspace administration node



Example configuration

You have several workspaces, with several clients that have access to one or more workspaces and they need appropriate file access for each workspace.

Nearly all workspaces are created with a client-specific name, e.g.:

- clienta_ws1
- clienta_ws2
- clientb_1
- clientb_2
- clientb_another_clientb_workspace
- clientc_a
- clientc_b

The client name forms the first part of the workspace ID. If there are several workspaces for the same client, an underscore separates the client name from the additional characters used to make each workspace ID unique.

Your file system has folders using the same client-specific name, e.g.:

- \\stagingarea\files\\clients\\
- \\stagingarea\files\\clients\\clienta
- \\stagingarea\files\\clients\\clientb
- \\stagingarea\files\\clients\\clientc

In this case, all workspaces and folders follow the same pattern. This allows you to define one file access pattern for multiple workspaces.

Placeholder extraction pattern

^(.+?)_.*
This pattern extracts the first part of the workspace ID, i.e., anything before the underscore.

Regex to limit file access

^\\\\stagingarea\\files\\clients\\{CLIENTID_FROM_WORKSPACEID}.

Root Directory

\\stagingarea\files\clients\{CLIENTID_FROM_WORKSPACEID}
Example: When a user works in workspace **clienta_ws2**, the placeholder extraction pattern will extract `clienta` from the workspace ID. This results in this allowed root directory: `\\stagingarea\files\clients\clienta`.

In case there are workspaces that do not allow use of a regular expression, you can define file path restrictions per workspace. In this example, it is the **prod_new_2** workspace.

In this example, the regular expression `.*` allows browsing in the complete file system. The root directory `\\stagingarea\files` suggests a starting point for browsing.

Tip: Try to create as few workspaces with non-standard workspace IDs as possible. This reduces configuration effort. Still, you can use the **Non-superuser file access in individual workspaces** table for workspaces introduced before this security feature was implemented.

Related:

https://en.wikipedia.org/wiki/Regular_expression

"Placeholder extraction pattern" on page 20

"Regex to limit file access" on page 20

"Root directory" on page 21

"Non-superuser file access in individual workspaces" on page 21

2.9 Workflow: Setup Security without Specified Superuser

Note: If you do not specify any superuser, all users with an Administrator user role are superusers and they automatically have access to all workspaces and filepaths.

Assume that you want only users with an Administrator user role to have access to all workspaces and to manipulate CORE Administration.

1. First you grant all people that should have Administrator, Configuration, Operator or Monitoring rights access to the **admin** application and assign the appropriate role.

   By default now all Administrators are superusers,and all users with Configuration, Operator or Monitoring roles are non-superusers.

2. To ensure users who do not have the Administrator role cannot manipulate CORE Administration:

   Create applications in workspaces that do not contain the **admin** application.

3. To ensure users who do not have the Administrator role only access the workspaces they really need:

   Create applications that these users administer or monitor in one workspace. Create applications administered or monitored by other users in different workspaces.

4. Grant the users access to applications in their specific workspaces.
5. Now make sure that these users only have access to filepaths that they need to access:

   Restrict file access in the **admin** application configuration.

Related:

" Restrict File Access" on page 12

2.10 Workflow: Security with Specified Superuser

One path to a secure system is that users get only access to the applications and workspaces they need. Others still need the full access granted by the Administrator role. How do you achieve this?

Assume you want only one user group, called **admingroup**, to have access to all workspaces and to manipulate CORE Administration:

1. First, split Administrators into superusers and non-superusers.

   To do so, in the **admin** application configuration, add the **admingroup** group name in the **List of supergroups**. Restart the **admin** application.

   This makes all other Administrators non-superusers. Users with the Configuration, Operator or Monitoring role are non-superusers by default.

2. Grant all people that should have Administrator, Configuration, Operator or Monitoring rights access to the **admin** application and assign the appropriate role.
3. To ensure that non-superusers cannot manipulate CORE Administration:

   Create applications in workspaces that do not contain the **admin** application

4. To ensure non-superusers only access the workspaces they really need:

   Create applications that these users administer or monitor in one workspace. Create applications administered or monitored by other users in different workspaces.

5. Grant the users access to applications in their specific workspaces.
6. Grant all non-superusers, i.e., Administrators, Operators etc., access to applications in their specific workspaces.
7. Now make sure that these users only have access to filepaths that they need to

access:

Restrict file access in the **admin** application configuration.

Related:

"Split Administrators into Superusers and Non-superusers" on page 9

" Restrict File Access" on page 12

2.11 Configure Security for CORE Administration

The configuration settings in CORE Administration are shown in the order they appear in the user interface.

.

2.11.1 Hide Explore Tab

Activate to hide the **Explore** tab in CORE Administration for all users, including super-users.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:

- true
- false

Default value:

- false

2.11.2 Forbid creation of command-line tasks

If this checkbox is active, no user can create a task of the **Execute Command Line** type on the **Scheduling** tab for an application.

Use this option to protect your system against fatal command line errors by inexperienced users.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- false

2.11.3 Forbid creation of command-line reports

If this checkbox is active, on the **Reports** tab for an application in CORE Administration, and in the Axcelerate Ingestion module, no user can create a command line report when they click **Create new report**.

Use this option to protect your system against fatal command line errors by inexperienced users.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- false

2.11.4 Allow internal settings with 'SHIFT'+configure

If this checkbox is active, all users can use the internal mode for configuration.

Note: If you deactivate the checkbox, you cannot undo deactivation without assistance from Recommind Support.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- true

2.11.5 Hide empty workspaces

If this checkbox is active, only superusers will see empty workspaces.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- false

2.11.6 Hide Hardware tab (Administration)

If this checkbox is active, non-superusers will not see the **Hardware** tab which is part of the **Monitoring** tab in CORE Administration.

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- false

2.11.7 Hide Hardware tab (ECA/Ingestion)

If this checkbox is active, no user will see the **Hardware** tab which is part of the **Monitoring** tab in the Axcelerate Ingestion module .

This setting is only visible in internal mode.

Location: **admin** application: **Visibility**

Allowed values:
- true
- false

Default value:
- false

2.11.8 List of superusers

When you add at least one user with Administrator role to this list, or an Administrator group name to the **List of supergroups**, the Administrator role is split into:

- superuser Administrators who can access all workspaces and functionality, and
- non-superuser Administrators who can only access specific workspaces.

If you leave both lists empty, all Administrators are superusers.

This setting is only visible in internal mode.

Location: **admin** application: **Cross workspace administration**

Allowed values: names of users with Administrator role

Default value:
- None

2.11.9 List of supergroups

When you add at least one Administrator group to this list, or an Administrator user name to the **List of superusers**, the Administrator role is split into:

- superuser Administrators that can access all workspaces and functionality, and
- non-superuser Administrators that can only access specific workspaces.

If you leave both lists empty, all Administrators are superusers.

This setting is only visible in internal mode.

Location: **admin** application: **Cross workspace administration**

Allowed values: names of user groups with Administrator role

Default value:
- None

2.11.10 Placeholder extraction pattern

Define the regular expression that allows you to extract the desired characters from the workspace ID. This pattern is used to fill in the CLIENTID_FROM_WORKSPACEID placeholder that can be used in the **Regex to limit file access** and **Root directory** fields, and in the **Non-superuser file access in individual workspaces** table.

Example: `^(.+?)_.*`

This setting is only visible in internal mode.

Location: **admin** application: **Cross workspace administration**

Allowed values: regular expression

Default value:
- None

2.11.11 Regex to limit file access

Define a file path pattern using a regular expression. This file path pattern defines the file access for all workspaces not listed under **Non-superuser file access in individual workspaces**. The regular expression can contain CLIENTID_FROM_WORKSPACEID which will be replaced with the value delivered by the **Placeholder extraction pattern**.

Example: `^\\\\stagingarea\\files\\clients\\{CLIENTID_FROM_WORKSPACEID}`

The limited file access applies to all non-superusers. If you leave this field empty, non-superusers will have access to the complete file system from CORE Administration.

This setting is only visible in internal mode.

Location: admin application: **Cross workspace administration > Default file access for non-superusers**

Allowed values: regular expression

Default value:
- empty

Related:

"Placeholder extraction pattern" on the previous page

2.11.12 Root directory

Root directory suggested to non-superusers when they click **Browse** in workspaces not listed under **Non-superuser file access in individual workspaces**. Placeholder {CLIENTID_FROM_WORKSPACEID} can be used, which will be replaced with the value delivered by the **Placeholder extraction pattern**.

The filepath entered here must match the **Regex to limit file access**.

This setting is not mandatory, but helps users to define a valid file access.

Example: `\\stagingarea\files\clients\{CLIENTID_FROM_WORKSPACEID}`

This setting is only visible in internal mode.

Location: admin application: **Cross workspace administration > Default file access for non-superusers**

Allowed values: filepath

Default value:
- empty

Related:

"Placeholder extraction pattern" on the previous page

2.11.13 Non-superuser file access in individual workspaces

Define file system access for individual workspaces. For all workspaces not mentioned in this table, the **Regex to limit file access pattern** is used to define file system access.

This setting is only visible in internal mode.

Location: **admin** application: **Cross workspace administration**

Workspace ID

Allowed values: Id of a workspace

Default value:
- None

Regex

Regular expression that defines the access to the file system from the given workspace. Placeholder {CLIENTID_FROM_WORKSPACEID}, defined in the **Placeholder extraction pattern** field, can be used in the regular expression.

The limited file access applies to all non-superusers. Leave empty to allow access to the complete file system.

Example: `.*`

Allowed values: regular expression

Default value:
- empty

Root Directory

Root directory suggested to all users when they click **Browse** in the given workspace. This setting is not mandatory, but helps to define a valid file access.

Placeholder {CLIENTID_FROM_WORKSPACEID} can be used, which will be replaced with the value delivered by the **Placeholder extraction pattern**. The directory must match the regular expression in the **Regex** column. Leave empty to not define a root directory.

Example: `\\stagingarea\files`

Allowed values: filepath

Default value:
- None

Related:

"Placeholder extraction pattern" on page 20

3 Best Practices for Application Creation

Before you create any application

Before you create your first application, it is useful to think about all the applications that you need to create, and which administrative staff should have access to them.

Do not create an application in the Default workspace

The default workspace contains the admin application that represents CORE Administration and lets you make changes to its security settings and features.
If you avoid creating a new application in this workspace, users that have no Administrator rights cannot access the workspace and cannot make changes to CORE Administration.
This makes the complete system more secure and reliable.

Put applications with similar administrative users into the same workspace

Operators and users with Configuration or Monitoring role can access any workspace that contains an application to which they are granted access.
If you create all applications for which specific users with Configuration, Operator or Monitoring role have access, into one workspace, these users will not have access to other workspaces, which protects the other workspaces against changes by unexperienced staff.

Related:

"User Roles for CORE Administration" on page 4

4 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.

5 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. Recommind, Axcelerate, Axcelerate Cloud, Axcelerate OnDemand, and CORE's name and logo are registered trademarks of Recommind, Inc.

Copyright