For end users

Registration

- When registering with an invitation, if the user that did the inviting no longer has permission to invite users then a specific error is now given to the person registering. Previously they would be shown a generic unauthorised error page with no information about why they couldn't proceed.

- When registering without an invitation, the system can now impose restrictions about what email address domains users are allowed to register from.

Tasks

- When viewing the index of tasks, the list of reasons for the task existing is now always shown after the task name with any comments about the task beneath. Previously if comments existed then the reasons would not be shown.

- When viewing a task, the information about it now separates the list of reasons why the task was created from any comments on the task.

Fixes

- Issues with lists in the HTML editor have been fixed.

- Corrections to the help system for some settings pages have been made.

- A small number of minor issues have been fixed.

For group administrators

Blog and space moderation

- Jiglu now supports pre-screening of blog posts, blog comments, discussion messages and knowledge entries for toxic content. This optional feature is provided by an external paid service – hosted customers should contact us for more information.

    - Contributions above the allowed level of toxicity will by default be sent to those with the *Group moderator* role for moderation. For blog posts, where there is no moderation stage, they will default to being sent back to the author for revision.

    - In the group workflow settings there are new settings for the action to take when a contribution is above the allowed level of toxicity.

- Pre-screening of contributions for banned words, such as profanity, has been extended to blog posts and knowledge entries. This provides a basic alternative to using toxicity screening.

    - Blog posts found containing banned words will default to being sent back to the author for revision. Knowledge entries will be sent to those with the *Group moderator* role for moderation.

    - In the group workflow settings there are new settings for the action to take when a blog post or knowledge entry is found to contain banned words.

- For blogs, there is a new *Blog workflow* settings category and new notifications for when a post is rejected or sent back to its author for revision.

- The workflow settings for discussion messages have been reorganised, splitting them into those to do with the content of a message and those to do with messages that came from email.

For system administrators

Registration

- When the system allows public access to user registration, you can now limit from what email address domains people are allowed to register using the *Allowed domains* setting in the *User workflow* system settings category.

Blog and space moderation

- The *Content filtering* system settings page has a new *Content toxicity level* setting with the percentage score above which contributions are treated as containing toxic content.

DMARC

- Jiglu previously had the option to change all email addresses in live discussion messages to local addresses in the system so as to work around issues with email servers rejecting mailing list messages due to DMARC validation. This has been extended in this version to allow you to choose what to do depending on the sender's domain's DMARC policy. For new installations and for upgrades when the setting was not previously turned on then the default will be to rewrite addresses only if the sender's DMARC policy is set to *reject*. For upgrades if the setting was previously turned on then addresses will always be rewritten. You can find the *Replace external From: address* setting in the *Email processing* group settings category if you wish to change the behaviour.

- Delivery failures due to DMARC rejection now have a lower impact on the score used to determine if a user should have their email deactivated, to lower the chance of this happening when their own email service is not at fault.

Non-delivery notifications

- The system log now contains entries for when a message could not be delivered to a user. This includes the delivery status code that was received, when available.

- Improvements have been made to the processing of non-delivery notifications, resolving some implementation inconsistencies with the email standards.

For operations engineers

Upgrade

- Changes to `bootstrap.properties` for properties used to configure AWS services will need to be integrated.

  - A single set of credentials is now used for all AWS services.

  - Jiglu now supports AWS authentication using the more secure EC2 instance profile credentials.

  - There is a new property `com.jiglu.contentAnalysis.toxicityAnalyser` to support the use of Amazon Comprehend for content toxicity analysis.

Other changes

- Third-party libraries have all been updated to their latest recommended versions.

Security

- Improvements have been made to webapp security, further restricting the resources that layer can access.

- There are no new security fixes in this release since 16.0.2.