For end users

- You can now transfer a knowledge entry to a discussion message in the same space. When you select the *Transfer* button there is a new option for this in the pop-up menu.
- When two-factor authentication is in use it wasn't previously possible to access feeds from the system that were not public and needed authentication. Access using your main account password could also be a security risk.

  You can now generate a separate password to use for feeds by going to *My preferences* and choosing the *Feed access* option. You will then be given a choice as to whether to generate a new password for private feeds, generate a new password for Atom Publishing Protocol use as well as private feeds, or revoke the existing feed password.
- When changing your account password, you will now be prevented from reusing a password that you have recently used. There may also be a limit on how many times you can change your password each day.
- When you create a new account or change your password, it is now explicitly disallowed to use a password that is too common or contains parts of your name, email address account, the system name or system hostname. In addition, you will now need a longer password with fewer repeating or ascending characters to have it scored more strongly.
- Cookies are now mandatory to use the system. Previously if cookies were disabled then session information would be stored on URLs but this could be a security risk.

Fixes

- Fix for a system error when accessing help pages if you did not have user administration rights.
- Fix for a system error if you attempted to add a tag with a date that was identical to one that already existed in the group.
- Fix for member profile pages giving a system error if the user does not have profile / view permission but does have member / view permission.
- Fixes for insufficient error handling for some invalid form fields or parameters.
- Fixes for system errors or broken presentation on some pages when accessing a resource at the same time as it was updated, deleted or had its permissions changed elsewhere.
- A number of minor issues have been fixed.

For group administrators

- The newsletter add and edit pages now only show the roles that are allowed to be used to target the newsletter.
- Tracking information is now removed from URLs in contribution text or from sources.
- There is additional validation of URLs from feeds and spidered sources, so some items that were previously dropped or caused issues on ingestion are now correctly processed.

For system administrators

- When the system is configured to permit users that have forgotten their password to get an email with a link to change it, the form to begin this process will give different responses depending on their account status. While more helpful to users, this allows the existence of usernames or email addresses to be discovered. If you do not want this to be possible then you can now have users given a generic message instead. To do this, go to the *User security* system settings category and change *Keep account existence secret* to *Yes*.
- There is a new setting in the *User security* system settings category for after how many changes of password a password can be reused. The default is 10.
- There is a new setting in the *User security* system settings category for how many times a user can change their password each day. The default is unlimited.
- The setting for how long a user has to change their password after requesting an email to do so has moved from the *User workflow* system settings category to *User security*.
- There is a new notification in the *User notifications* system settings category for the email notification that is sent to a user when they change their feed password.
- Activity logs will contain new events for when a feed password is changed by a user, when a feed logs on and when a feed log on failed.
- If you log off from extra system administrator rights and you are currently on a system settings page you will now be returned to your radar home page.

For operations engineers

- Jiglu now has an oauth2 server available at */+auth*. The permitted domains are set using the *com.jiglu.oauth.clientDomains* property in the *bootstrap.properties* configuration file. When not configured the page will return a page not found error.
- There is a new password blocklist file containing passwords that may not be used in */etc/jiglu/ passwords-blocklist.conf*. By default, this is the top 10,000 passwords over 8 characters in length taken from the NCSC's pwned passwords list.
- An issue reading the *signature-patterns.conf* configuration file for detecting signatures in incoming discussion emails has been resolved.
- Event plugins can now listen on any resource or event type.
- Third-party libraries have all been updated to their latest recommended versions.

Security

- A potential denial of service attack vector causing service agents to fail due to insufficient validation of URLs when adding or editing a source has been closed. A user would require administration privileges in a group to have been able to exploit this. Additional validation of URLs has been added throughout the product at both webapp and API level.