Implementing SaaS Security Workflows in JIRA Software

DoControl.

The DoControl Impact

DoControl provides comprehensive data access security that adds a foundational layer of preventative controls to protect sensitive business-critical data and files in JIRA. The solution integrates with JIRA to secure all shared data and files accessed by every identity and entity, both internal employees as well as 3rd party collaborators. DoControl's fine-grain data access controls help prevent data overexposure and exfiltration, automatically remediate the risk of insider threats, and allow for business enablement to be achieved in a secure way.

Integrate JIRA with DoControl to:

Gain Visibility and Control

JIRA lacks the visibility required to manage and control access for groups and domains that regularly manipulate and share sensitive company data. The number of users and assets within a standard JIRA implementation is unmanageably high, creating a scalable problem when attempting to secure data and files within the application. Gaining insight into which boards/projects contain PII term, info, or labels and gaining comprehensive visibility into issues and their sub-entities, such as comments, descriptions, and attachments. In order to maintain control of these inputs, organizations must monitor and enforce compliance with relevant policies and procedures. With DoControl enabled teams can enable near real-time monitoring of every user activity to detect and respond to immediate threats PII and sensitive data leaks.

Establish Secure Workflows

DoControl provides future-proofed, secure workflows for specific JIRA users and groups that present higher-levels of risk to the business. Establishing permissions to JIRA users lacks the required granularity to implement effective data access control policies. Applying settings that are based on specific users and departments, or other similar relevant parameters, is not supported in JIRA. For example, customer success and support teams are more likely to share sensitive information within boards/projects. JIRA lacks the ability to apply specific workflow policies to different groups and departments. Company-wide data access policies also lack granularity, and are limited to generic CRUD (create, read, update and delete). Currently in JIRA there is no ability to remove a publicly shared document.

Key Benefits

1. Gather insights and data from users interactions in near real-time from events that take place in JIRA projects
2. Gain full visibility into JIRA project specific issues and their sub-entities, such as comments, descriptions, and attachments
3. Establish secure workflows that are future-proofed to mitigate the risk of data overexposure and exfiltration
4. Centrally enforce consistent data access controls throughout JIRA, and all other critical SaaS applications

This poignant issue could be the impetus that leads to a significant data breach. DoControl provides users with the ability to delete an entire issue with all sub-entities, such as the issue's comments, attachments, and descriptions.

Initiate Automated Notifications

Automated notifications can be triggered to individual actors or security teams regarding policy violations, or PII that was detected with issues as well as sub-entities. Discovering policy and PII within the JIRA admin console can be challenging, especially as most teams leveraging JIRA have a significant amount of data in boards/projects. DoControl provides the ability to distribute automated notifications whenever an issue becomes detected, enabling organizations to take a risk-based approach to securing files within JIRA. Policies can be set to distribute specific notifications based on risk. For example, lower risk events can notify the individual actor, and higher risk events can be directed to Security teams to respond to. Automating this process frees up time for IT and Security teams to focus on more strategic projects, as well as improving the general 'security mindedness' of business users through ongoing interaction and engagement.

DoControl can address limitless security policy violations or PII within JIRA, as the platform is completely-event driven by all SaaS activity within the application. Once defined, secure data access policies will be triggered in near real-time, adding a critical layer of preventative controls to minimize data leakage.

Enforcement Actions

Enforcement actions can be established by defining secure workflow policies that trigger automatically by events within JIRA. For example: If a Jira user in your organization adds PII in the issue description or in a comment, your security team can receive a notification in near real-time and take appropriate action.

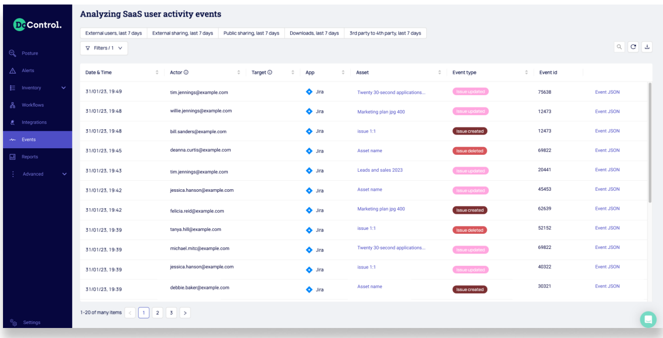
Reach out to a DoControl expert to review additional enforcement actions and threat model coverage. DoControl provides a rich catalog of playbooks that can be leveraged to create specific enforcement actions. Policies can be created from scratch, or the playbooks can be adjusted to align to specific security program requirements. Creating secure workflow policies for JIRA with DoControl can be achieved in a few simple clicks. The playbooks can be found directly within the DoControl console by accessing the Workflows tab.

Permission Scopes

A full listing of required read/write permissions scopes are available in the DoControl documentation portal, which you can find on our user guide. Integrating DoControl with JIRA requires a Basic Plan, and the integrator must be a 'JIRA Administer for the Cloud site' OR 'Administer Jira'

1. From the DoControl side menu, click Integrations.
2. Under the Jira icon, click Connect. The Connect to JIRA Wizard then opens.
3. Click "Let's go" and follow the instructions in the wizard.
4. Click Allow to grant DoControl access permissions.
5. Select which Jira sites DoControl should retrieve information from. When finished, the wizard indicates that Jira is connected.

Once integrated, the DoControl solution is enabled to automatically implement the enforcement actions that've been pre-established (examples listed above), across all JIRA users and assets. The DoControl solution is enabled to enforce automated remediation actions within the JIRA environment such as deleting issue and sub-entities such as comments and attachments.



Analyzing SaaS user activity events

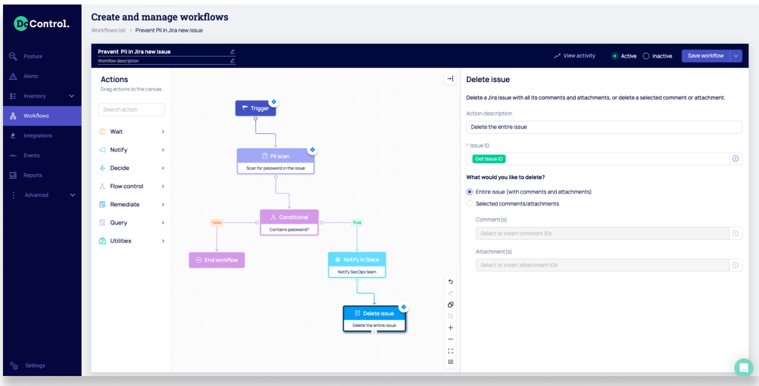
External users, last 7 days | External sharing, last 7 days | Public sharing, last 7 days | Downloads, last 7 days | 3rd party to 4th party, last 7 days

Filters / 1

Date & Time	Actor	Target	App	Asset	Event type	Event id	
31/01/23, 19:49	tim.jennings@example.com		Jira	Twenty 30-second applications...	Issue updated	75638	Event JSON
31/01/23, 19:48	willie.jennings@example.com		Jira	Marketing plan jpg 400	Issue updated	12473	Event JSON
31/01/23, 19:48	bill.sanders@example.com		Jira	issue 1:1	Issue created	12473	Event JSON
31/01/23, 19:45	deanna.curtis@example.com		Jira	Asset name	Issue deleted	69822	Event JSON
31/01/23, 19:43	tim.jennings@example.com		Jira	Leads and sales 2023	Issue updated	20441	Event JSON
31/01/23, 19:42	jessica.hanson@example.com		Jira	Asset name	Issue updated	45453	Event JSON
31/01/23, 19:42	felicia.reid@example.com		Jira	Marketing plan jpg 400	Issue created	62639	Event JSON
31/01/23, 19:39	tanya.hill@example.com		Jira	issue 1:1	Issue deleted	52152	Event JSON
31/01/23, 19:39	michael.mitc@example.com		Jira	Twenty 30-second applications...	Issue updated	69822	Event JSON
31/01/23, 19:39	jessica.hanson@example.com		Jira	issue 1:1	Issue updated	40322	Event JSON
31/01/23, 19:39	debbie.baker@example.com		Jira	Asset name	Issue created	30321	Event JSON

1-20 of many items < 1 2 3 >

DoControl provides a consolidated view of all JIRA events, assets, and more



Create and manage workflows

Workflows list > Prevent PII in Jira new issue

Prevent PII in Jira new issue

Workflow description

● Active ○ Inactive

Delete issue

Delete a Jira issue with all its comments and attachments, or delete a selected comment or attachment.

Action description: Delete the entire issue

* Issue ID: Get issue ID

What would you like to delete?

● Entire issue (with comments and attachments)

○ Selected comments/attachments

Comment(s): Select or insert comment IDs

Attachment(s): Select or insert attachment IDs

Establish secure workflows for specific JIRA users and groups that present higher-levels of risk to the business

About JIRA

JIRA is a software application developed by the Australian software company Atlassian that allows teams to track issues, manage projects, and automate workflows. One of the most popular open source testing software tools – JIRA is trusted by over 65,000 companies worldwide, including giants like Spotify, Cisco, eBay, Square and Airbnb. This issue tracking tool is mainly used to track, organize and prioritize issues, bugs, features and tasks related to software and mobile apps.JIRA Software is a powerful platform that combines issue collection and agile project management capabilities into a single application. The platform leverages all kinds of project management skills, including software development, Agile project management, bug tracking, scrum management, content management, marketing, professional service management, and so much more.

Partner with DoControl and start moving security closer to what drives the modern business forward. Learn more.