# Preventing customer information leaks from Jira filter /dashboard sharing

- What's the problem?
- Background: shared filters and dashboards
- Locking down sharing
  - Remove the ability to share with anonymous users
  - O Remove the ability to share with all logged-in users
  - Remove group sharing
- Cleaning up from oversharing
- Conclusion

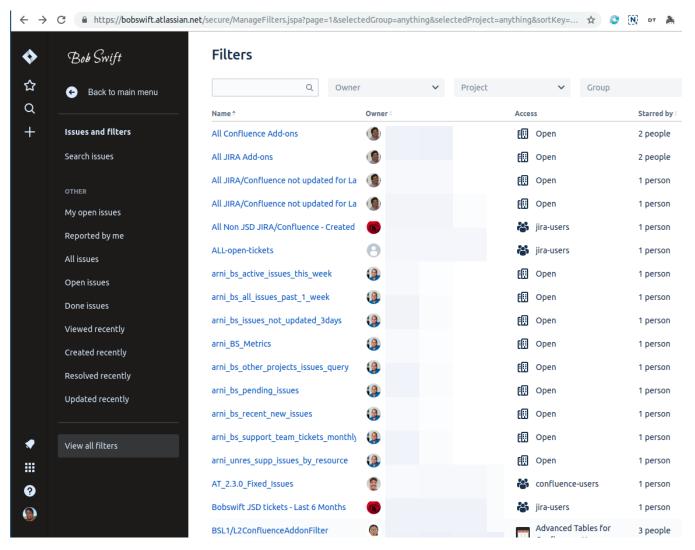
## What's the problem?

Say you run a public Jira instance for interacting with customers. Customer A representatives can view project A, Customer B representatives can view project B, and so on. Your company's employees can see all customer projects.

Jira allows users to share saved searches (filters) and dashboards amongst themselves. We would like to let Customer A representatives create their own filters and dashboards, shared amongst themselves and also with our employees.

Jira allows sharing out-the-box, but with one flaw: when you're trying to completely partition customers, **Jira's sharing tends to leak customer names** and filter/dashboard names. Customer A can potentially see the names of Customer B's filters and dashboards, and their owners

You can see this on most public Jira instances by going to the 'Find Filters' (server) or 'Issues and filters' (Cloud) page. For example:



# Background: shared filters and dashboards

Why are these lists of filters visible on public instances anyway?

By default all users have the Created Shared Object global permission:

### **Create Shared Objects**

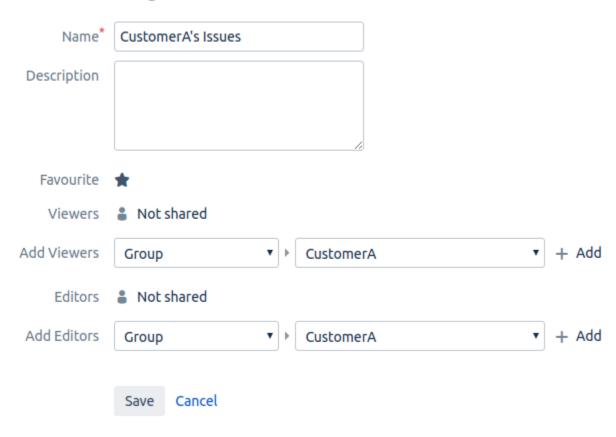
Ability to share dashboards and filters with other users, groups and roles.

- users
  - View Users Delete
- jira-users

View Users Delete

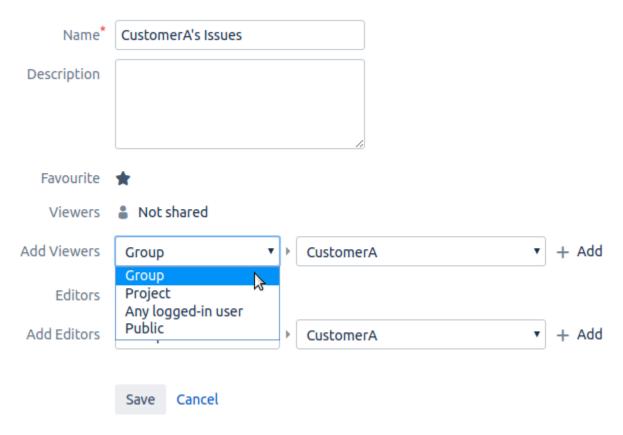
This allows Customer A to create filters shared with other users in their group:

## Edit Current Filter ③



Unfortunately it also allows Customer A to *overshare* their filter, either to "Any logged-in user", which would include members of other companies, or to "Public", which means anyone, even users not logged in to Jira:

## Edit Current Filter ②



One quite legitimate solution to prevent oversharing is to prevent sharing at all. Just deny customers the **Create Shared Object** global permission. This is what Atlassian have done on <a href="https://jira.atlassian.com">https://jira.atlassian.com</a>. It solves a lot of problems.

But say you do want to allow customers to create their own custom dashboards and filters, and share them amongst themselves and with you. Perhaps only because it's now a relied-upon feature in your customer base..

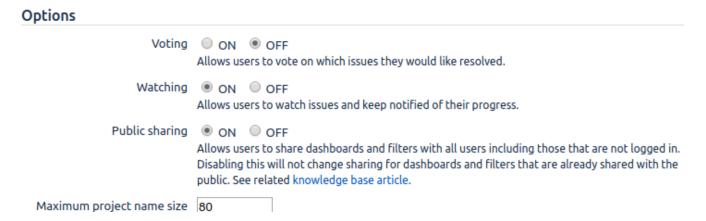
It is possible to allow safe sharing, but requires some Jira tweaking.

# Locking down sharing

Down the rabbit hole we go...

#### Remove the ability to share with anonymous users

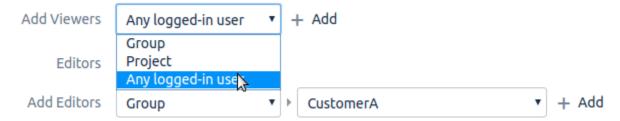
Atlassian have (as of JIRA 7.2.2) added a 'Public sharing' General Configuration option:



This gets rid of the 'Public' option.

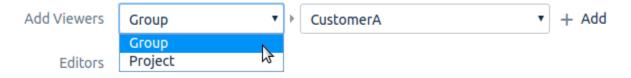
#### Remove the ability to share with all logged-in users

We're still left with the possibility of Customer A creating a 'CustomerA's Issues' filter made visible to Customer B by picking 'Any logged-in user'



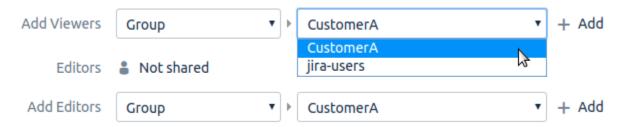
Getting rid of 'Any logged-in user requires tweaking a JSP, namely atlassian-jira/template/aui/edit-share-types.jsp:

The 'Any logged-in user' option is now gone:



#### Remove group sharing

We also want to get rid of the Group sharing option, at least for customers:



Sharing by group can only lead to unhappiness:

- If the customer shares with jira-users, they're exposing their filter to other customers.
- If the customer shares with CustomerA, then our employees can't see the filter, because they aren't in CustomerA group.

So we need to remove the 'Group' option as well, but only for customers, not employees. Here is the complete change to atlassian-jira/template/aui/edit-share-types.jsp:

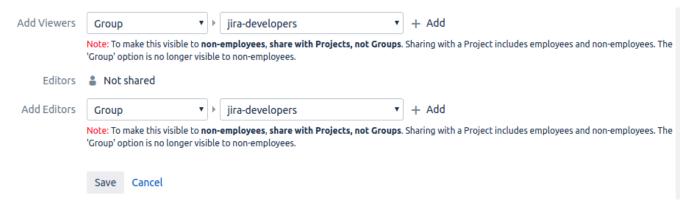
diff --git a/atlassian-jira/template/aui/edit-share-types.jsp b/atlassian-jira/template/aui/edit-share-types.jsp --- a/atlassian-jira/template/aui/edit-share-types.jsp

```
+++ b/atlassian-jira/template/aui/edit-share-types.jsp
@@ -34,11 +33,39 @@
                         <select class="select medium-field" id="share_type_selector_<ww:property value="</pre>
parameters['mode']"/>">
                             <ww:iterator value=".">
                                 <ww:if test="./available == true">
                                     < -- BEGIN CUSTOMIZATION: Hide the 'group' option from non-employees, and
'Any logged-in user' option from everyone --%>
                                     <%@ page import="com.atlassian.jira.user.ApplicationUser"%>
                                     <%@ page import="com.atlassian.jira.security.groups.GroupManager" %>
                                     <%@ page import="com.atlassian.jira.security.JiraAuthenticationContext" %>
                                     <%@ page import="webwork.action.ActionContext" %>
                                     <%
                                         final GroupManager groupManager = ComponentAccessor.getGroupManager();
                                         final JiraAuthenticationContext jiraAuthenticationContext =
ComponentAccessor.getJiraAuthenticationContext();
                                         final ApplicationUser user = jiraAuthenticationContext.getUser();
                                         boolean isEmployee = groupManager.isUserInGroup(user, "MyCompany") | |
groupManager.isUserInGroup(user, "administrators");
                                         ActionContext currentContext = ActionContext.getContext();
                                         request.setAttribute("isEmployee", isEmployee);
                                     %>
                                     <ww:if test="./shareType != 'group' || @isEmployee == true">
                                     <ww:if test="./shareType != 'loggedin'">
                                     <%-- END CUSTOMIZATION --%>
                                     <option value="<ww:property value="./shareType"/>"><ww:property value=".</pre>
/shareTypeLabel"/></option>
                                     <%-- BEGIN CUSTOMIZATION. --%>
                                     </www:if>
                                      </www:if>
                                     <%-- END CUSTOMIZATION --%>
                                 </www:if>
                             </www:iterator>
                         </select>
                         <ww:iterator value="." status="'typeStatus'">
                         <%-- BEGIN CUSTOMIZATION. --%>
                         <ww:if test="./shareType != 'group' || @isEmployee == true">
                         <ww:if test="./shareType != 'global' && ./shareType != 'loggedin'">
                         < -- END CUSTOMIZATION --%>
                         <span class="share_select" id="share_<ww:property value="./shareType"/>_<ww:property</pre>
value="parameters['mode']"/>" <ww:if test="@typeStatus/first == false">style="display:none"</ww:if>>
                             <ww:property value="./shareTypeEditor" escape="false"/>
                             <ww:if test="./addButtonNeeded == true">
@@ -53,8 +80,17 @@
                                 </span>
                             </www:if>
                         </span>
                         <%-- BEGIN CUSTOMIZATION. --%>
                         </www:if>
                         </www:if>
                         <%-- END CUSTOMIZATION --%>
                         </www:iterator>
                         <div class="fieldDescription" id="share_type_description_<ww:property value="parameters</pre>
['mode']"/>"></div>
                         <-- BEGIN CUSTOMIZATION: the div below if our addition to explain the limited sharing
option to users. --%>
                         <div class="fieldDescription"><ww:if test="@isEmployee == true"><span style="color:</pre>
red">Note:</span> To make this visible to <b>non-employees</b>, <b>share with Projects, not Groups</b>. Sharing
with a Project includes employees and non-employees. The 'Group' option is no longer visible to non-employees.
/ww:if></div>
                         < -- END CUSTOMIZATION --%>
                         </www:if></div></div>
                 <ww:if test="parameters['editEnabled'] == false"></div></ww:if>
             </div>
```

Now customers can only share by Project:



while employees have the option to share by group or project, but are advised to share things with customers by project:



# Cleaning up from oversharing

If your Jira has allowed over-sharing for a while now, you are in a bit of a pickle. Jira doesn't allow even administrators to edit filters they don't own (

JRASERVER-41269 - Getting issue details... STATUS

). Your best option is to:

- Find the extent of the problem through Jira's Shared filters and Shared dashboards admin pages.
- If the number of over-shares is small, for each shared object: temporarily 'become' the owner and change the share to a specific project or projects.
- If the number of over-shares is large, you are best off using SQL to tweak the sharepermissions table. You might like to contact us for help, as we have done this before.

## Conclusion

JIra enables filter/dashboard sharing by default which, while normally a good thing, often leads to information leaks in situations where you need strict compartmentalization of users. We have provided some JSP tweaks to provide more sharing flexibility than Jira natively supports.