

Metadata-Based Security

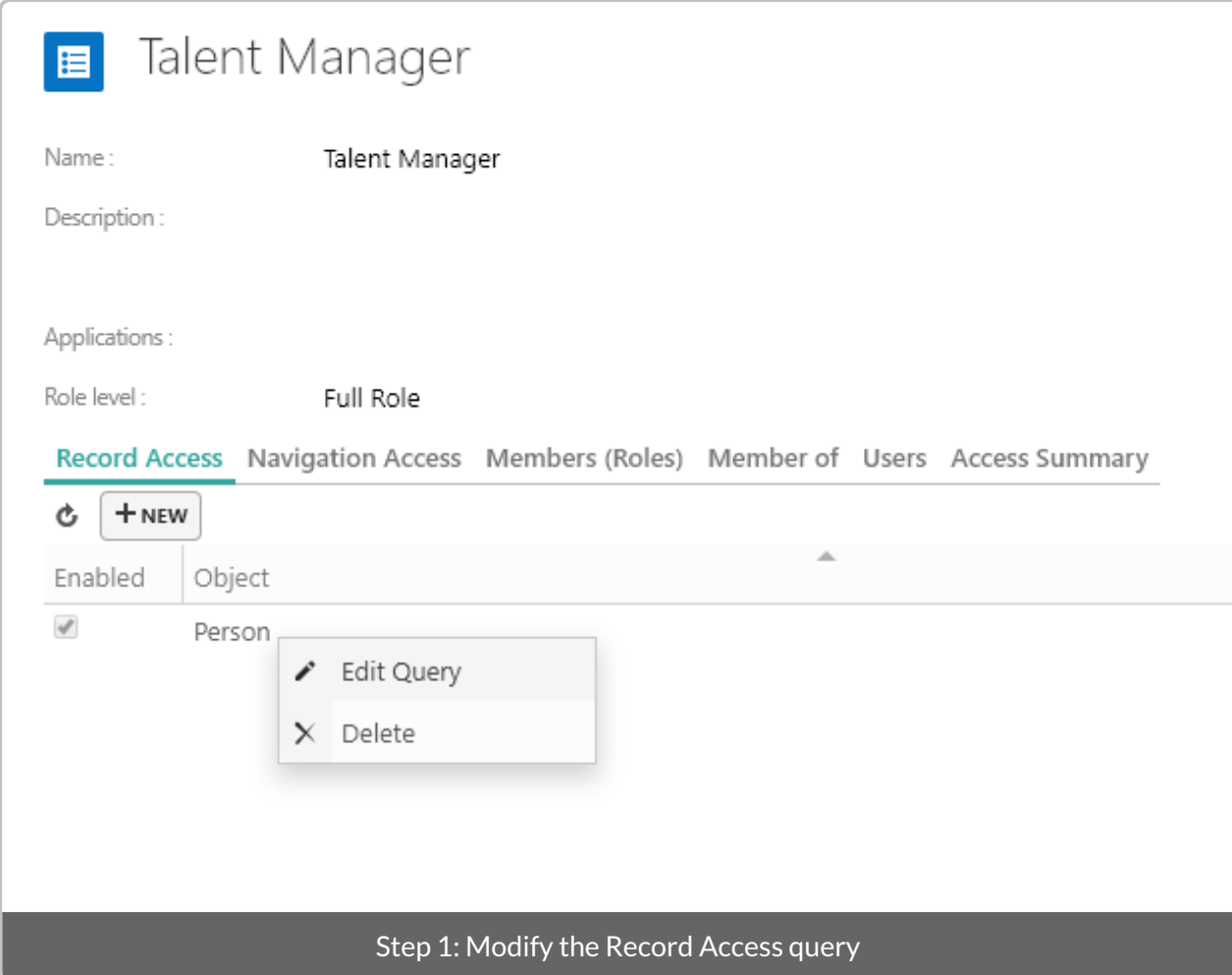
Last Modified on 31/05/2019 4:19 pm AEST

User roles can leverage metadata-based security, which is the ability to secure objects based on metadata. This is done by selecting the **Edit Query** option for **Record Access** and configuring the security as desired.

Example

Step 1

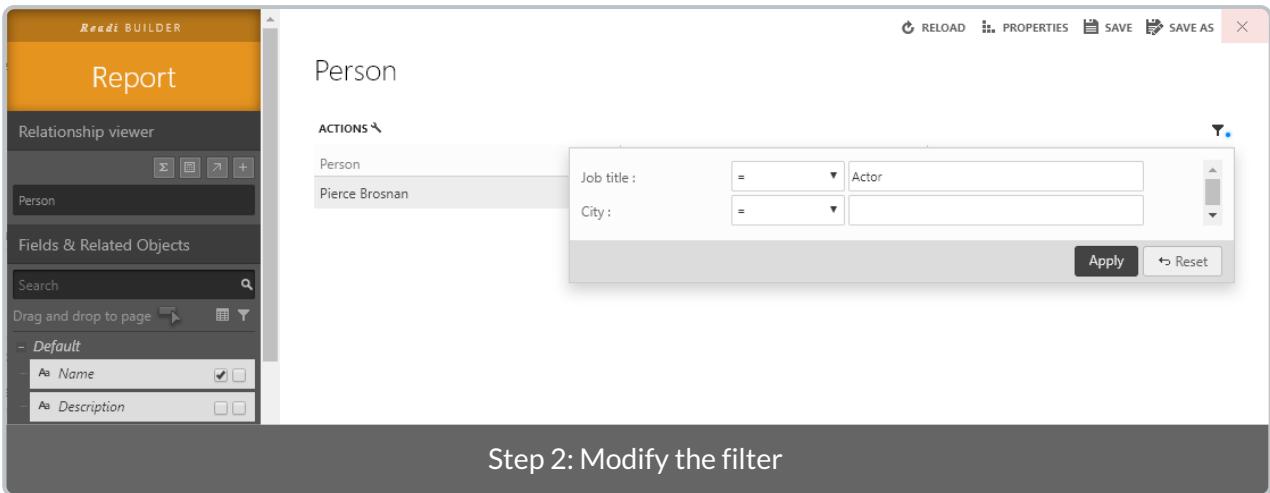
Navigate to **User Roles** in the security administration, and open a role that needs to be configured.



The screenshot shows the 'Talent Manager' interface. At the top, there is a header with a menu icon and the text 'Talent Manager'. Below this, there are several fields: 'Name : Talent Manager', 'Description :', 'Applications :', and 'Role level : Full Role'. A navigation bar contains tabs: 'Record Access' (highlighted), 'Navigation Access', 'Members (Roles)', 'Member of', 'Users', and 'Access Summary'. Below the tabs, there is a '+ NEW' button and a table. The table has two columns: 'Enabled' and 'Object'. The first row has a checked checkbox in the 'Enabled' column and 'Person' in the 'Object' column. A context menu is open over the 'Person' row, showing two options: 'Edit Query' (with a pencil icon) and 'Delete' (with an 'X' icon). At the bottom of the screenshot, a dark grey bar contains the text 'Step 1: Modify the Record Access query'.

Step 2

A report appears, where the filter can be edited; modify the filter and save.



Step 3: Test

While other users can view the full list of contacts, signing in with the talent manager role will only show Pierce in the list.

