

Managing Field Visibility

On the page:

- [Permissions](#)
- [Manage Fields](#)
- [Delete Extracted Fields](#)

Related pages:

- [Roles and Permissions](#)
- [Analytics and Data Security](#)

This topic describes how to manage the visibility of fields in your analytics data. This capability enables you to hide fields that you don't want other people in your organization to see.

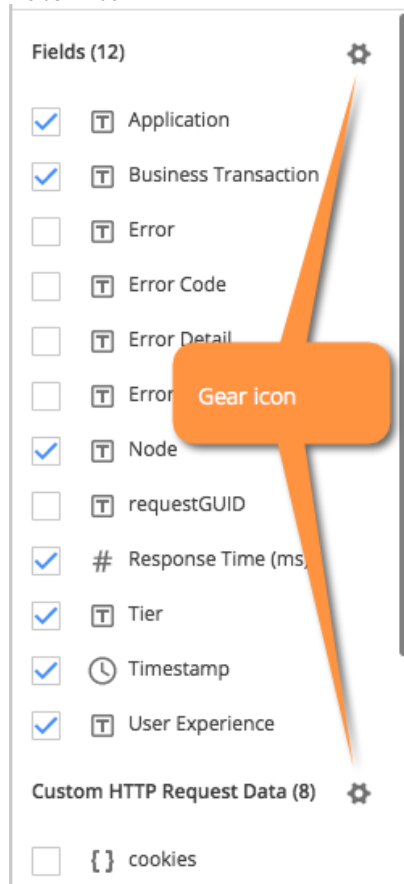
You can set the visibility of the fields in most of the analytics events types with the exception of custom events. Hiding fields in custom events is not supported.

Permissions

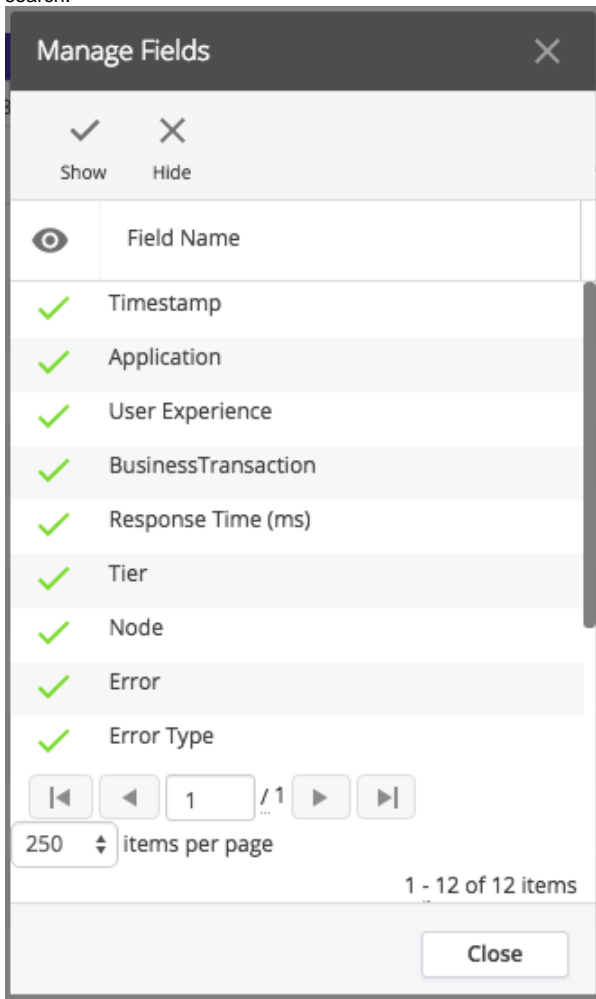
The Manage Fields permission is required to manage field visibility. If a role has the Manage Fields permission, it means all the users with that role can manage all the fields they have access to. They can unhide the fields or see which fields have been hidden. For instance, if you have "Manage Fields" permission and "Transaction" permission" for the application "Ecommerce App" then you can only see and manage fields for that application.

Manage Fields

1. From the Analytics Search window find and click the gear icon (⚙️) that appears near each **Fields** grouping to open the Manage Fields window:



2. Use the Manage Fields window to show or hide fields as needed. The list of fields varies depending on the event type selected for the search.



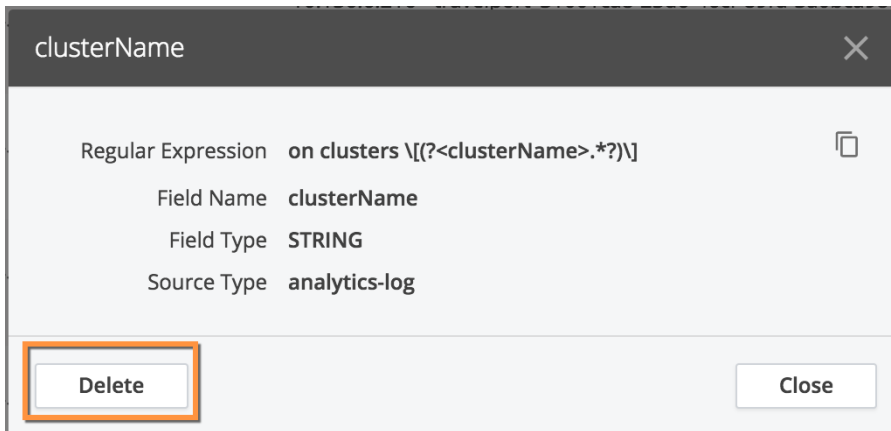
Delete Extracted Fields

In 4.3, you may have two types of extracted fields, fields created in 4.2 where the controller version has been upgraded to 4.3 and fields extracted from logs with log source rules.

For fields created in 4.2, you can delete the fields using these steps:

1. Hover (with the cursor) over the field and click on the view icon that appears.

2. Click on **Delete** in the popup.



For fields being extracted from logs using log source rules, you can delete the fields by editing the source rules. See [Field Extraction for Source Rules](#).