Analytics and Data Security

Related pages:

- Managing Field Visibility
- Managing API Keys
- Roles and Permissions

Application Analytics provides role-based access control (RBAC) to enable you to control and protect your data. The Analytics permissions enable you to provide granular, controlled access to features and analytics data in your environment. This topic outlines the available permissions.

Roles and Permissions

A predefined role called Analytics Administrator is provided with preset permissions for all Analytics-specific permissions.

You can clone predefined roles as a starting point for creating your own customized roles, but you should not assume the cloned roles have all of the permissions of the predefined role. In some cases, there may be hidden permissions, so you should add or remove permissions as needed for your customized role to ensure that you get the RBAC result you need.

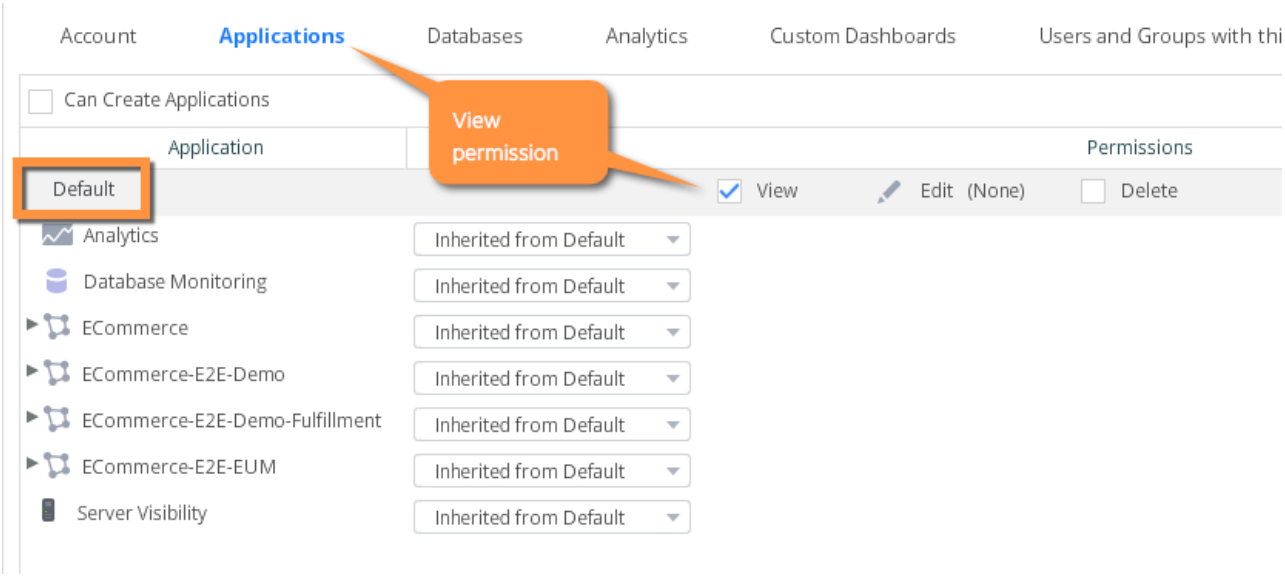
To create roles and assign users to roles for Analytics, users need both the **Analytics Administrator** and the **Account Owner** role.

Also, see Business iQ Analytics Permissions.

Default Application

To ensure that your users have access to the full Analytics functionality they need, be sure to give them the view permission on the Default Application. This permission is given to all predefined admin roles and to the read-only role, **Applications & Dashboards Viewer**. If you create new roles for analytics, you need to grant this permission in addition to specific analytics permissions.

When you create a new role, this permission is not automatically given to that role. You can either turn on the view permission by checking the **V iew** option on Default Application or you can add the read-only role to new users. From the Administration page Applications tab, grant view permissions to the Default Application as shown in the following screenshot:



Analytics Administration UI Tabs

Access the Analytics tab in the Controller Administration UI when creating new roles to see the available permissions.

General Permissions

This section contains permissions that control access to analytics features:

- Manage Fields
- Manage APIs
- Manage Metrics
- Configure Log Analytics with Source Rules
- Manage Business Journeys
- Manage Experience Levels

Search Permissions

All the saved searches created in Analytics appear in this section. The admin role can assign View, Edit and Delete permissions on a search by search level. The admin can create and save specific searches needed by various roles in your organization. In addition to enabling the permissions, View, Edit, and Delete, for a specific saved search, the admin must also enable access to the related application or log source type for the search. Otherwise, the data access level won't be granted to the role.

To create a new saved search, the user must have the **Can Create a Search** permission.

View permission: Assigning only the View permission for a saved search means users can not edit or delete the search.

Edit permission: Assigning Edit permission for a saved search means users can modify the filter criteria and save back to the same search.

Delete permission: Assigning Delete permission for a saved search means users can delete the search.

Event Type Permissions

Transactions Permissions: This section enables the admin user to assign permissions for viewing application transaction data. Permissions can be granted to view all transaction data for the account or on an application by application basis. When creating new roles, remember that granting permissions to view transaction analytics data does not automatically grant permissions to see all application data associated with a specific transaction analytics record. You need to grant at least read-only permissions to the application to enable the user to see associated transaction snapshot data such as flow maps.

Log Permissions: This section enables the admin user to assign permissions for viewing log data. Permissions can be granted to view log data for all source types configured for the account or on a source by source basis.

Browser Requests Permissions: This section enables the admin user to assign permissions for viewing browser request data. Permissions can be granted to view data for all applications for the account or for specific applications.

Mobile Requests Permissions: This section enables the admin user to assign permissions for viewing mobile requests and crash report data. Permissions can be granted to view data for all applications for the account or for specific applications.

Custom Analytics Events: This section enables the admin user to assign permissions for querying custom analytics events data. Permissions can be granted to view data for all custom analytics events or for specific applications.

Synthetic Permissions: This section enables the admin user to assign permissions for querying Synthetic events data. Permissions can be granted to view data for all applications for the account or for specific applications.