Application Permissions

On this page:

Related pages:

- Roles and Permissions

You can set application permissions for custom roles from the Applications tab in the Controller Administration UI. You can assign the Can Create Applications permission to a custom role.

Application permissions follow an inheritance model. There are three levels in the model listed here in order from highest (default) to lowest (tier-specific):

- Default permissions
- Application-wide permissions
- Tier-specific permissions

By default, each level inherits from the one above it, unless you customize permissions at a lower level. This mechanism enables you to grant access to groups or users for specific business applications in the Controller UI.

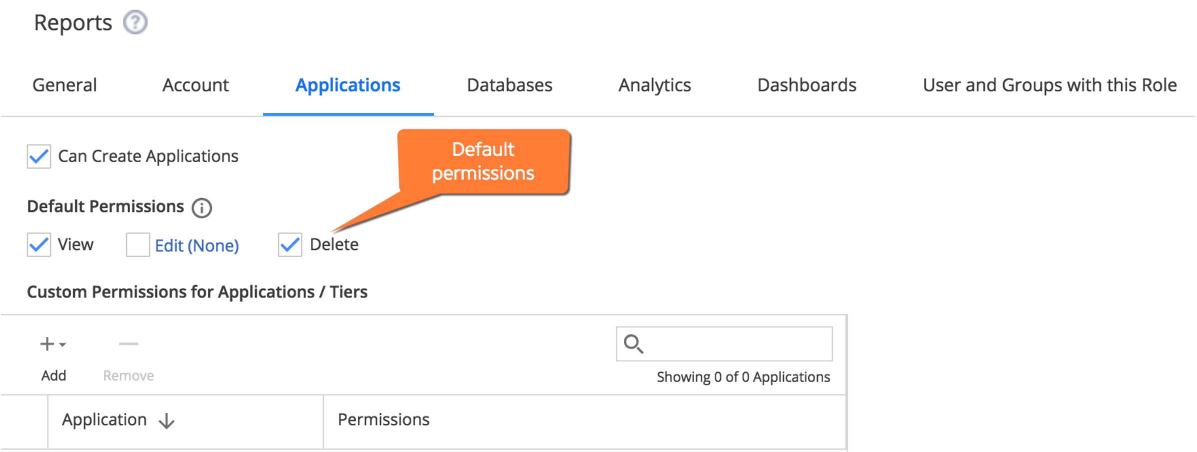
Customized permissions at a specific level override more general permissions at another level. That is, tier-specific permissions take precedence over application-specific permissions, and application-specific permissions override default permissions. Not all permissions can be customized at the tier-level.

Create Default Permissions

All new applications inherit default permissions.

To configure default application permissions

1. From the Controller Administration UI, add or edit a custom role for which you want to grant default application permissions.
2. On the Applications tab, to grant the role permission to create new applications, click **Can Create Applications**.
3. Under Default Permissions, select the default permissions for this role: **View**, **Edit** or **Delete**.



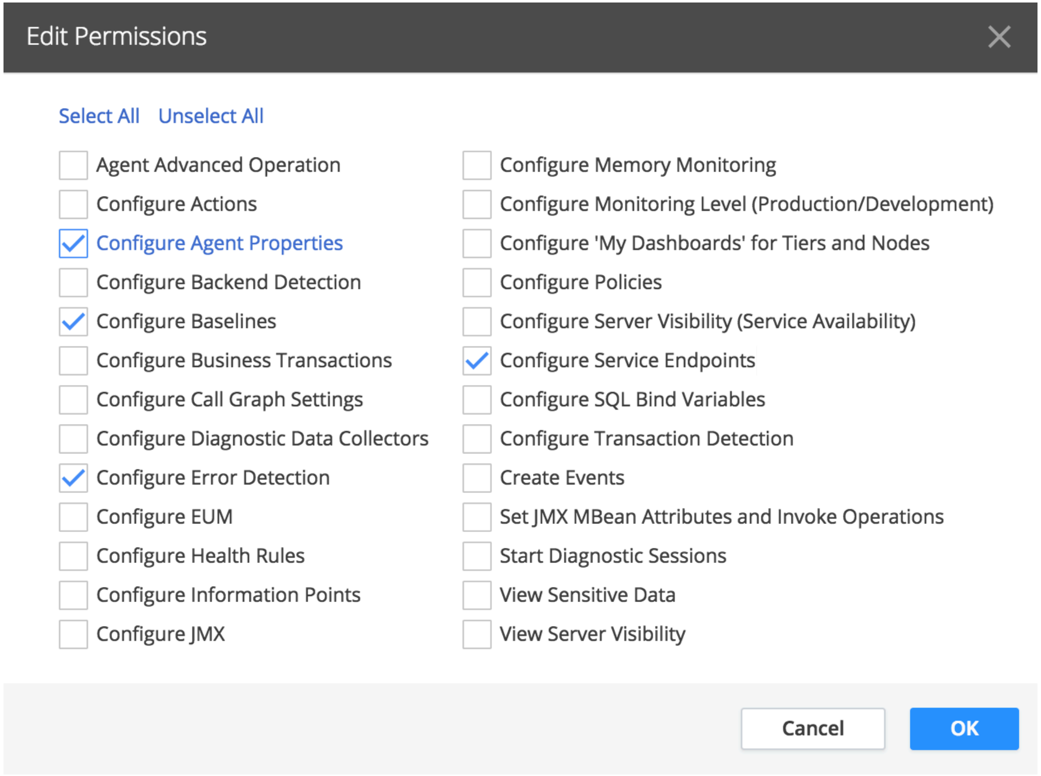
☑ Can Create Applications

Default Permissions

☑ View □ Edit (None) ☑ Delete

Default permissions
Custom Permissions for Applications / Tiers
Add
Remove
Showing 0 of 0 Applications
Application
Permissions

- Check **Delete** to grant permissions to delete any application. To grant permission to delete a specific application, customize the permission at the application level.
- To grant specific permissions to edit specific application configurations for all applications:
    i. Click **Edit** to give all permissions to all applications or deselect **Edit**, and then **click Edit(None)**.
    ii. In the Edit Permissions window select the permissions for this role.



□ Agent Advanced Operation
□ Configure Actions
☑ Configure Agent Properties
□ Configure Backend Detection
☑ Configure Baselines
□ Configure Business Transactions
□ Configure Call Graph Settings
□ Configure Diagnostic Data Collectors
☑ Configure Error Detection
□ Configure EUM
□ Configure Health Rules
□ Configure Information Points
□ Configure JMX
□ Configure Memory Monitoring
□ Configure Monitoring Level (Production/Development)
□ Configure 'My Dashboards' for Tiers and Nodes
□ Configure Policies
□ Configure Server Visibility (Service Availability)
☑ Configure Service Endpoints
□ Configure SQL Bind Variables
□ Configure Transaction Detection
□ Create Events
□ Set JMX MBean Attributes and Invoke Operations
□ Start Diagnostic Sessions
□ View Sensitive Data
□ View Server Visibility

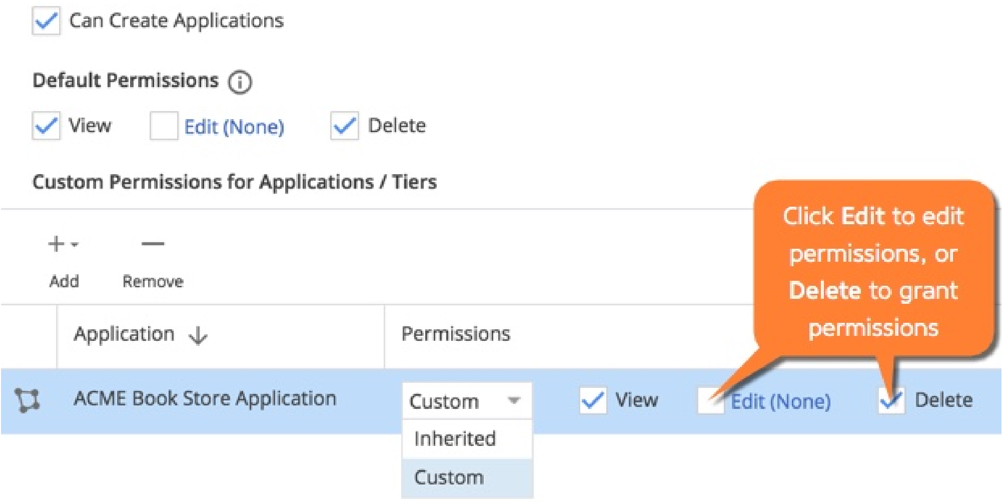
For information about the permissions that can be granted at the application level and tier levels, review the Application and Tier Level Permissions table.

4. Click **OK** in the Edit Permissions window.
5. Click **Save** at the top of the pane to save the configuration for this role.

Customize Application Permissions

To customize business application level permissions, follow these steps:

1. Choose **Custom** from the Permissions menu for the application (replacing the value of Inherited).
2. Check **View** option and then **Edit(None)**, as shown in the following screenshots. You can also grant permission to delete a specific application.



☑ Can Create Applications

Default Permissions ⓘ

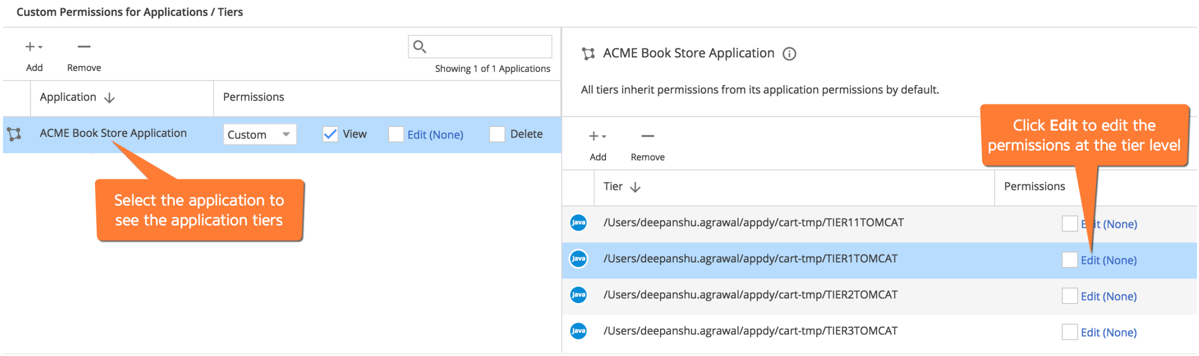
☑ View □ Edit (None) ☑ Delete

Custom Permissions for Applications / Tiers

Application	Permissions			
ACME Book Store Application	Custom	☑ View	□ Edit (None)	☑ Delete

Click **Edit** to edit permissions, or **Delete** to grant permissions

To customize permissions at the tier level, expand the application permission tree and click **Edit**.



Custom Permissions for Applications / Tiers

Application	Permissions			
ACME Book Store Application	Custom	☑ View	□ Edit (None)	□ Delete

Select the application to see the application tiers

ACME Book Store Application ⓘ

All tiers inherit permissions from its application permissions by default.

Click **Edit** to edit the permissions at the tier level

Tier ↓	Permissions
/Users/deepanshu.agrawal/appdy/cart-tmp/TIER11TOMCAT	□ Edit (None)
/Users/deepanshu.agrawal/appdy/cart-tmp/TIER1TOMCAT	□ Edit (None)
/Users/deepanshu.agrawal/appdy/cart-tmp/TIER2TOMCAT	□ Edit (None)
/Users/deepanshu.agrawal/appdy/cart-tmp/TIER3TOMCAT	□ Edit (None)

3. In the dialog box, choose the individual permissions for the selected tier and click **OK**.
4. Click **Save** when you are finished selecting permissions.

Overlapping Role Permissions Examples

Within specific and default permissions, granting a specific permission takes precedence over denying the same permission elsewhere. So, if a user is assigned two roles and one grants a permission and the second role denies it, the user will have permissions for the activity.

The following examples are designed to illustrate how overlapping permissions of different roles interact. The examples enable view, edit, and delete permissions to applications as shown for two Groups. The last column shows the resulting permissions for a specific user with roles that are assigned to each group.

Group 1			Group 2	
	Default Permissions (view, edit delete all applications)	**Explicit permissions (view, edit delete application-1)**	**Default Permissions (view, edit delete all applications)**	**Explicit permissions (view, edit delete application-1)**
A	None	Yes	Yes	None
B	Yes	None	Yes	Yes

C	Yes	None	None	None

- Result for example A: User has view, edit, and delete permissions to all applications, including application-1.
- Result for example B: User has view, edit, and delete permissions to all applications, including application-1.
- Result for example C : User has view, edit, and delete permissions to all applications, excluding application-1.

General Permissions

Permission	Activities Enabled	More Information
Can Create Applications	Create business, browser, and mobile applications. Also controls the Archive Snapshot action.	Business Applications
View, Edit and Delete permissions for new applications can be set as part of the default permissions for a custom role	View, edit or delete business applications (and the tier s and nodes), browser and mobile applications. Setting default delete permissions allows the user to delete all three artifacts from the application model.	Business Applications Tiers and Nodes

Application and Tier Permissions

You can grant the following permissions as specified. Permissions that can be customized at the tier level are indicated in the Description column. Asterisks (*) in the permissions table indicate permissions that are considered sensitive for security and data privacy purposes. Carefully consider the security and data privacy policies of your organization before granting these permissions.

Permission	Description of Activities Enabled	More Information
Configure Transaction Detection*	Create, edit, or delete transaction detection - can be at the tier level.	Transaction Detection Rules
Configure Backend Detection	Create, edit, or delete backends - can be done at tier level.	Backend Detection Rules
Configure Error Detection	Create, edit, or delete error detection.	Error Detection
Configure Diagnostic Data Collectors*	Create, edit, or delete diagnostic data collectors.	Data Collectors
Configure Call Graph Settings	• Edit call graph settings (no SQL) • Turn on or off capture raw SQL (call graph and SQL bind must both be on)	Call Graph Settings
Configure JMX	Create, edit, or delete JMX metrics.	Configure JMX Metrics from MBeans
Configure Memory Monitoring	Configure which custom classes are tracked by Object Instance Tracking. Note: To enable or disable Object Instance Tracking, you need the Configure Agent Properties permission.	Object Instance Tracking for Java
Configure EUM (for Browser RUM)	See End User Monitoring Permissions	Configure the Controller UI for Browser RUM

Configure EUM (for Mobile RUM)	See End User Monitoring Permissions	Configure the Controller UI for Mobile RUM
Configure Information Points*	Create, edit, or delete information points	Information Points
Configure Health Rules	Create, edit, or delete health rules	Configure Health Rules
Configure Actions	• Create, edit, or delete actions on agent properties UI • Create, edit, or delete email digests	Alert and Respond Actions Email Digests
Configure Policies	Create, edit, or delete policies.	Configure Policies
Configure Business Transactions	• Organize Business Transactions including: ◦ Group business transactions ◦ Exclude/un-exclude business transactions ◦ Delete business transactions ◦ Enable business transaction lockdown ◦ Rename business transactions • Configure business transaction thresholds • Configure snapshot settings • Set as a background task • Configure data collectors • Enable End User Monitoring • Enable analytics for business transactions • Enable or disable GUID injection	Organize Business Transactions Transaction Thresholds Transaction Snapshots Monitor Background Tasks Data Collectors Set Up and Access Browser RUM Collect Transaction Analytics Data Business Transaction and Log Correlation
Configure Baselines	Create, edit, or delete baselines.	Dynamic Baselines
Configure SQL Bind Variables*	Turn on or off capture raw SQL (also requires Configure Call Graph Settings).	Call Graph Settings
Configure Agent Properties	• Create, edit, or delete agent configuration (can be done at tier level). • Enable or disable automatic leak detection (can be done at tier level). • Enable or disable object instance tracking (can be done at tier level). • Enable or disable custom memory structure (can be done at tier level).	App Agent Node Properties Object Instance Tracking for Java Custom Memory Structures for Java
Agent Advanced Operation	• Reset agent from the node dashboard. • Request agent thread dumps. • Request agent debug logs.	Manage App Agents Diagnostic Actions Request Agent Log Files
Set JMX MBean Attributes and Invoke Operations	Edit MBean attributes or invoke actions on operations.	Monitor JMX
Configure Service Endpoints	Create, edit, or delete service endpoints.	Service Endpoint Detection
Configure Monitoring Level (Production/Deployment)	Switch between production and development mode.	Development Level Monitoring

Configure 'My Dashboards' for Tiers and Nodes	Create, edit or delete custom dashboards (can be done at tier level).	Create and Manage Custom Dashboards and Templates Custom Dashboards
Create Events	Create, edit, or delete events.	Alert and Respond API
Start Diagnostic Sessions	Start a diagnostic session.	Diagnostic Sessions
View Sensitive Data*	In combination with the Configure Transaction Detection permission, enables the use of Live Preview and Business Transaction Discovery features to stream live data from your application.	Custom Match Rule Live Preview