Configure Policies

On this page:

Related pages:

- Policies
- Monitor Events
- Health Rules
- Troubleshoot Health Rule Violations
- Actions
- Cloud Auto-Scaling

There are two ways to configure policies:

- Use the Policy Setup Wizard for simple policies that just send an email notification when a health rule is violated.
- Use the Manual Policy Wizard for anything more complicated.

Permissions

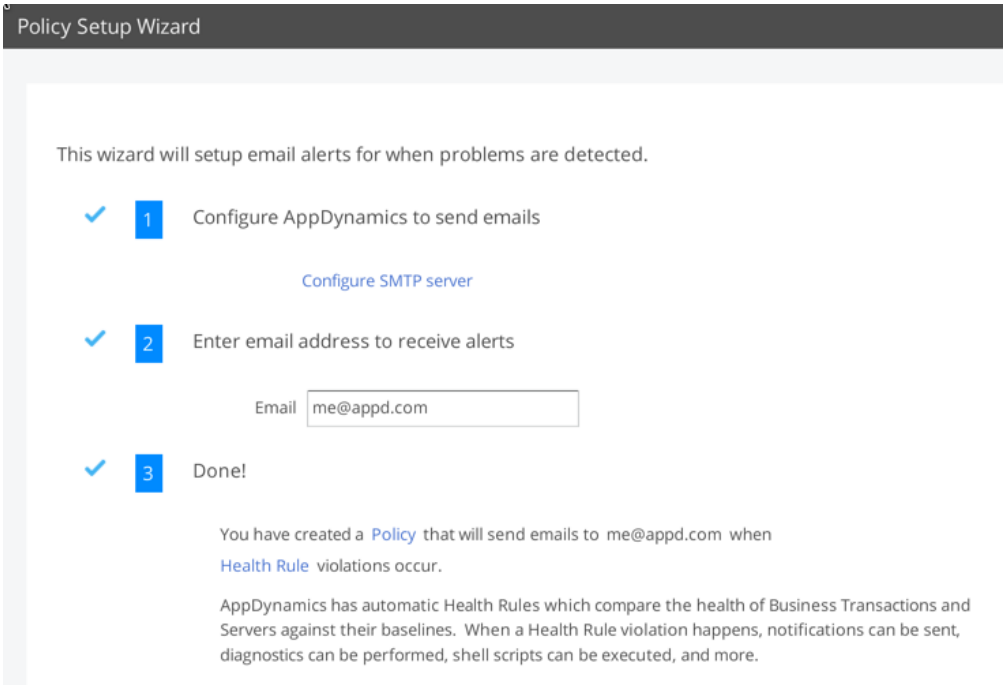
To configure policies, you need the **Configure Policies** permission.

Policy Setup Wizard

For simple policies, in the Controller UI, click **Alert & Respond > Policies > Policy Setup Wizard**.

To create a notification policy, you must set up an SMTP server (see Enable an Email Server) and supply an email address.

The policy is then created:



You can modify the policy later the same way you modify a policy that is created manually.

Manual Policy Wizard

The Manual Policy Wizard contains two panels:

- Trigger: Sets the events that trigger the policy, entities that are affected by the policy
- Actions: Sets the actions to take when the policy is triggered.

In either panel you can configure the policy name, enabled status, and whether to batch the actions executed by the policy.

To configure policies:

1. Click **Alert & Respond** in the menu bar.
2. Click **Policies** either in the right panel or the left navigation pane.
3. Select the context for the policy (specific Application, User Experience, Databases, Servers, or Analytics) from the pulldown menu.
4. Do one of the following:
    - To create a new policy, click the **Create Policy** (+) button.
    - To edit an existing policy, select the policy and click the.
    - To remove an existing policy, select the policy and click the **Delete** (-) button.

You can also copy, enable or disable a policy by clicking the appropriate button.

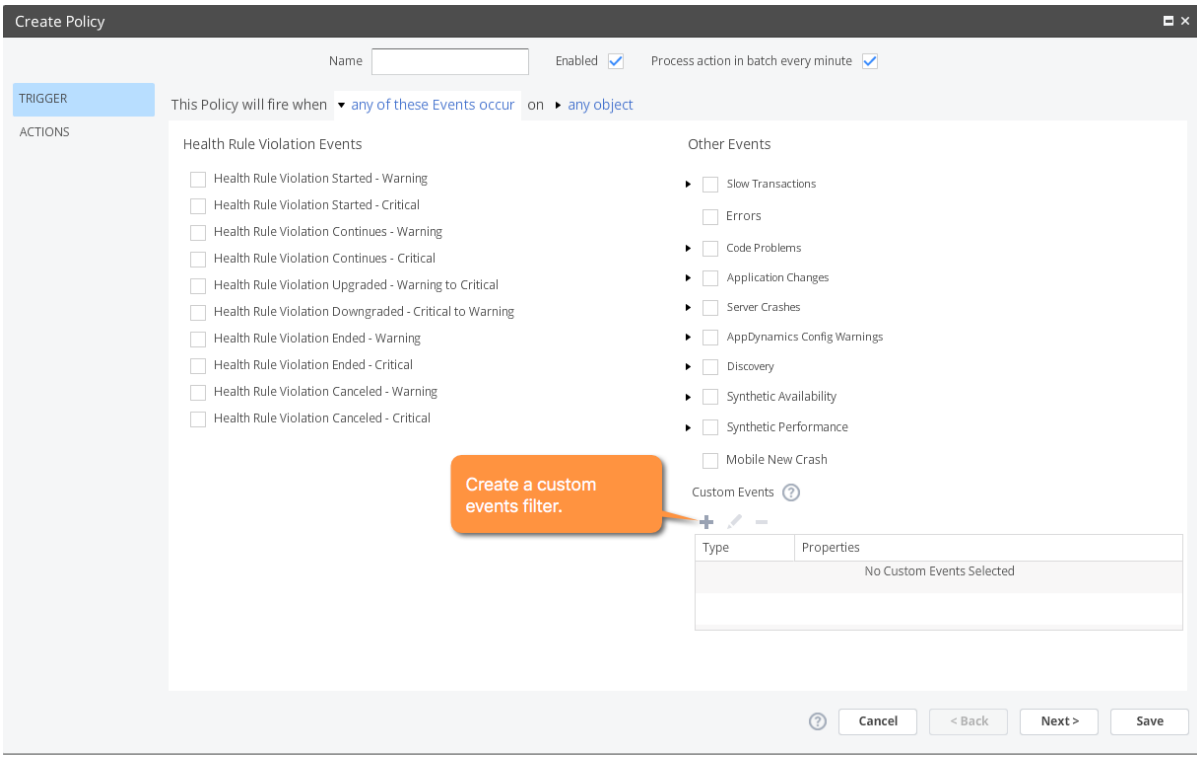
Configure Policy Triggers

The policy trigger panel defines the events and objects that cause the policy to fire and invoke its actions.

For policy triggers that depend on health violation events, the health rules must be created before you can create a policy on them. See Health Rules and Troubleshoot Health Rule Violations.

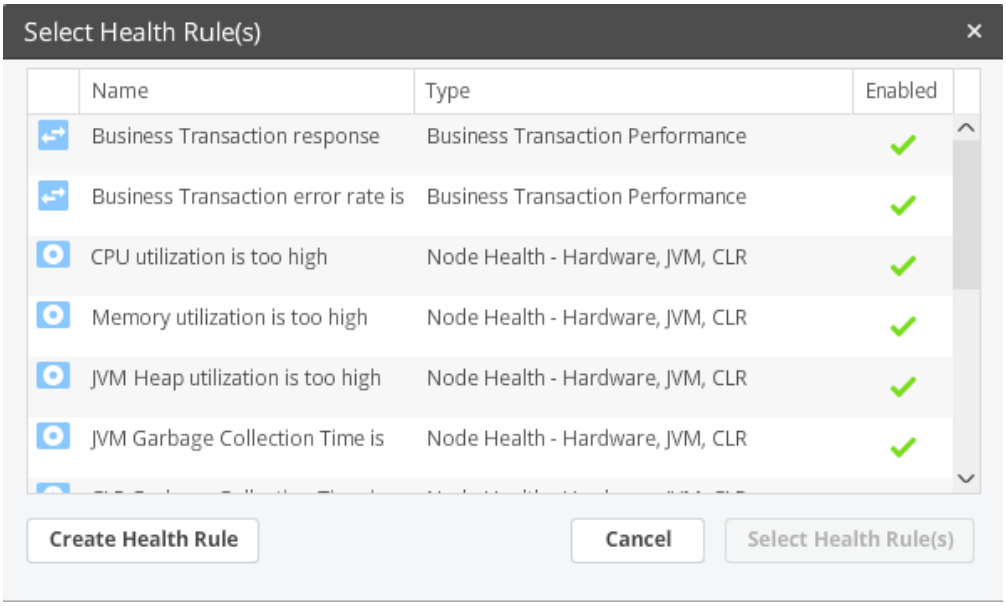
To configure policy triggers:

1. Click **Create Policy** (+ button) or select a policy and click **Edit** (pencil button).
2. Enter a name for the policy in the **Name** field.
3. To enable the policy, check the **Enabled** check box. To disable the policy, clear the **Enabled** check box.
   You can also enable or disable a policy by selecting it in the policy list and clicking the Enable or Disable button.
4. If you leave the **Process action in batch every minute** check box clear, the policy fires its actions immediately for every triggering event. If you check this check box, the policy fires its actions once for all the triggering events that occurred in the last minute. See "Policy Actions in Batch" in Policies.
5. On the left, click **TRIGGER** if it is not already selected.
6. Check the type of event(s) that should trigger the policy. You may need to click the arrow to expose specific events within an event category.
   If you check at least one health rule violation event, you can choose whether any (that is, all) health rule violation or only specific health rule violations will trigger the policy.

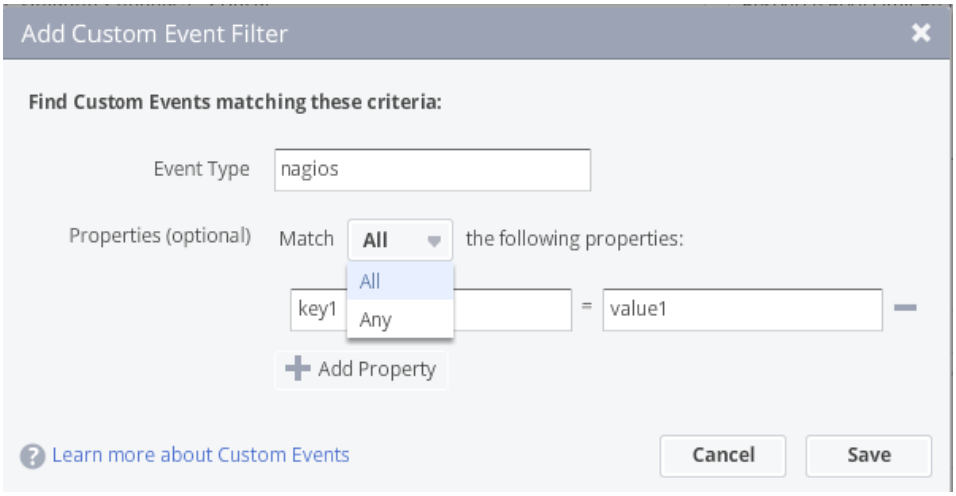


If your AppDynamics environment includes browser synthetic monitoring, you will see additional other events for Synthetic Availability and Synthetic Performance. See "Alerting and Synthetics" in Browser Synthetic Monitoring.

To designate specific health rule violations to trigger the policy, select These Health Rules, click the "+" icon, and then choose the health rules from the embedded health rule browser. You can also click **Create Health Rule** to create a new health rule as the trigger for this policy.



You can optionally designate specific custom events to trigger the policy, using the Custom Events panel in the lower right corner. Click the "+" icon.

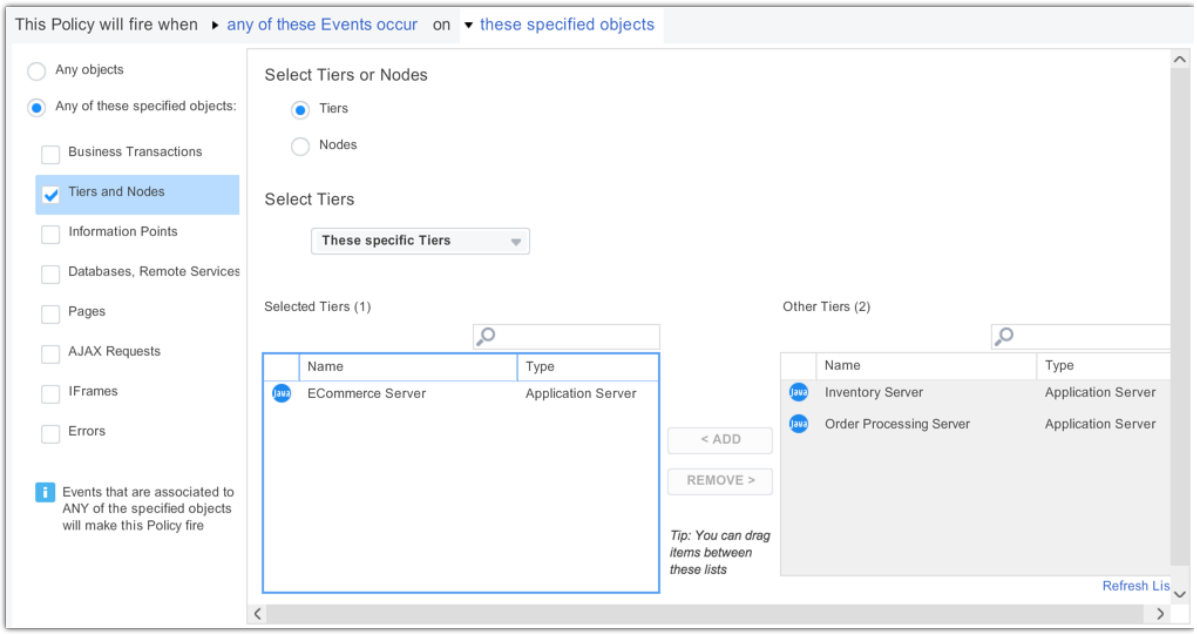


Specify the custom event type. Optionally add particular properties on that event as key/value pairs. For **Any**, at least one property must exist and match. For **All,** all properties must exist and match.

7. When you have finished selecting the events that trigger the policy, click **any object** to configure which objects to monitor for those events to trigger the policy.

If you select **Any Object**, the policy will be triggered by the configured events when they occur on any object in your application.
To restrict the policy to specific objects, select **Any of these specified objects** and then choose the objects.
For example, the following policy fires when selected events occur on the the ECommerce Server tier. You can similarly restrict

the objects to specific nodes, business transactions, Ajax Requests, and so forth.



You can restrict the affected nodes on the node name, on the type of node (Java, .NET, etc) on nodes in certain tiers, or on criteria such as meta-info, environment variables, and JVM system environment properties. Meta-info includes key value pairs for:

- key: supportsDevMode
- key:ProcessID
- key: appdynamics.ip.addresses
- any key passed to the agent in the appdynamics.agent.node.metainfo system property

To trigger by Health Rule Violation Events, leave the selection at **Any object**. Selecting **Any of these specified objects** mea ns that only non-health rule events — slow transactions, errors, and so forth — trigger the policy.

8. Click **Save**.

Configure Policy Actions

The policy actions panel binds an action to the trigger. It defines which actions the policy automatically initiates when the trigger causes the policy to fire.

The actions must be created before you can create a policy that fires them. See Actions and the documentation for individual types of actions (notification actions, remediation actions, etc.) for information on creating an action.

To configure policy actions:

1. If you have not already done so, open the policy wizard and edit the policy to which you want to add actions. See To access the Policy Wizard.
2. On the left, click **ACTIONS** if it is not already selected.
3. Click "**+**" icon. The list of existing actions appears. The available actions vary depending on the product area selected for the policy, such as Applications, Servers, Databases and so on.
   You can filter the list by checking the check boxes for the types of actions you want to see.
4. In the list of actions, select the action that you want this policy to execute and click **Select**.
   If you do not see an appropriate action for your needs, click **Create Action**. For information on creating actions, see Actions. Af ter you have created the action, select it here to assign it to the policy that you are configuring.
5. Click **Save**.

You can optionally test whether your action will be fired using the event simulation tool before you enable the policy in production.