

## Automated Workflows

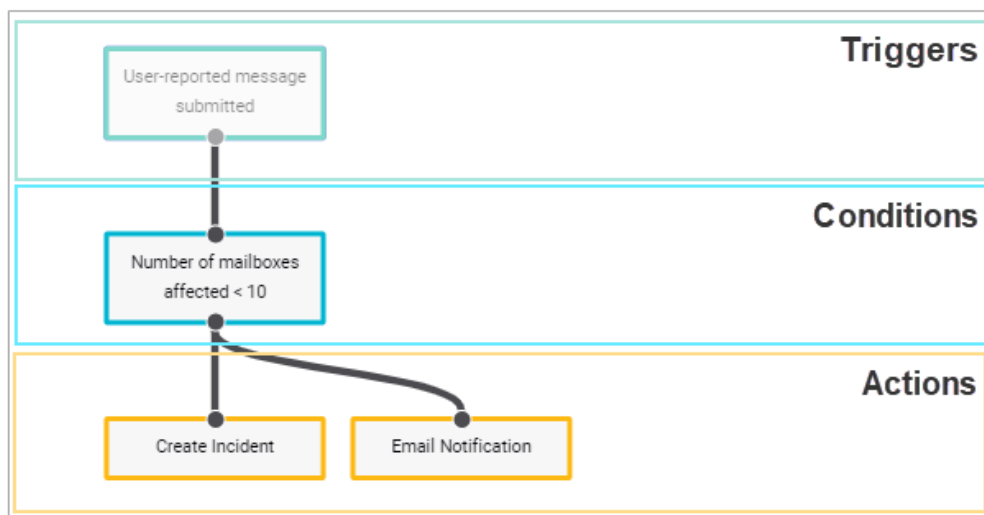
<https://campus.barracuda.com/doc/95263320/>

This functionality is available only with Barracuda Email Protection [Premium](#) and [Premium Plus](#) plans. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

Automated workflows enable you to take actions when certain events occur – automatically. You set up a workflow, then Incident Response automatically follows through, taking the actions you specify, without requiring further interaction from you.

Automated workflows consist of the three components:

- **Triggers** – The activity that sets the workflow in motion.
- **Conditions** – Optional. The status or value that must be met to continue the workflow. Based on the condition, the workflow travels through different paths. The conditions available are based on the trigger type.
- **Actions** – The outcome of the workflow. Specify the details of each of these actions in the Settings. Refer to [Automated Workflows Settings](#).



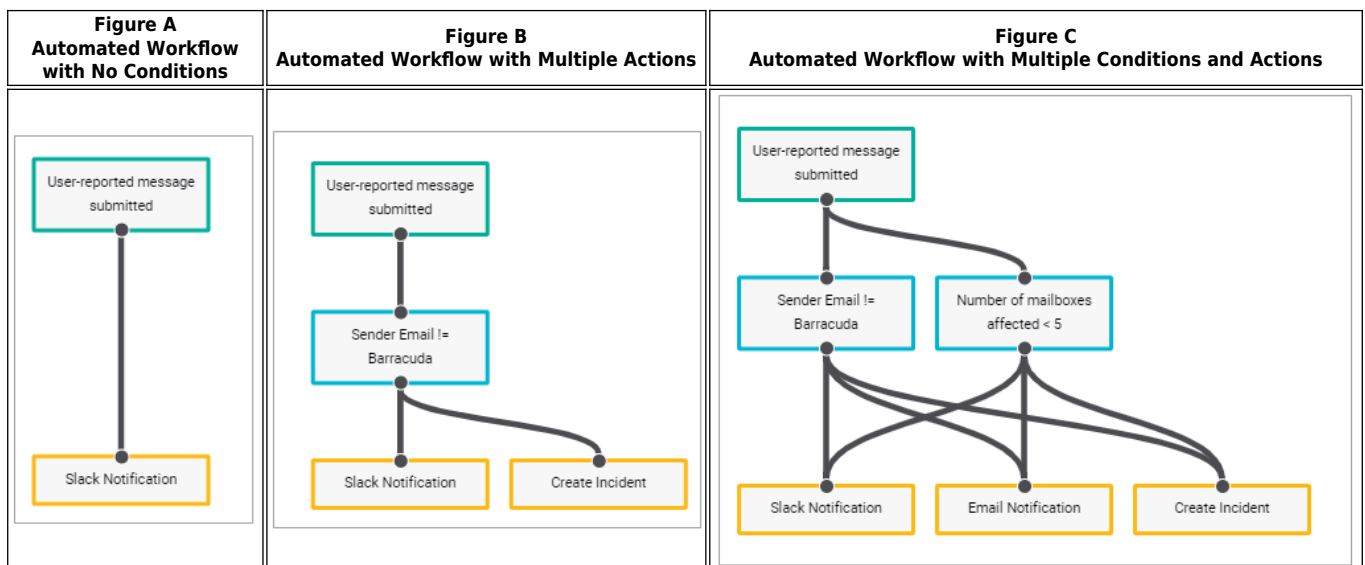
The following table describes the currently-available triggers, along with their associated conditions and actions. Conditions in **bold** indicate conditions specific for the associated trigger.

Triggers	Conditions (optional)	Actions
----------	-----------------------	---------

<p><b>Potential incident detected</b></p> <p>Prerequisite:</p> <ul style="list-style-type: none"> <li>Incident Response created a Potential Incident, as described in <a href="#">Potential Incidents</a>.</li> </ul>	<ul style="list-style-type: none"> <li>Email subject – Subject of the email involved in the Potential Incident.</li> <li>External/Internal email – Whether the email originated outside of or within your organization.</li> <li>Number of emails detected – How many emails are detected in the Post-Delivery or Related Threat.</li> <li>Number of mailboxes affected – How many mailboxes are affected by the potential incident. Note that this number might increase if you are still experiencing a malicious email attack.</li> <li><b>Post-delivery threat</b> – Based on Barracuda Networks' intelligence on currently circulating threats, threats that might already be present in your inbox.</li> <li><b>Related threat</b> – Threats based on an incident you already created.</li> <li>Sender country – Where the email originated.</li> <li>Sender email – Sender of the email involved in the Potential Incident.</li> </ul>	<ul style="list-style-type: none"> <li>Create incident – Creates an incident, based on the trigger and condition.</li> <li>Create email notification – Alerts administrators about this trigger, using the email specified in Automated Workflows Settings.</li> <li>Create Slack notification – Alerts administrators about this trigger, using the Slack webhook specified in the Automated Workflows Settings.</li> <li>Create Microsoft Teams notification – Alerts administrators about this trigger, using the Microsoft Teams webhook specified in the Automated Workflows Settings.</li> </ul>
<p><b>Sender Policy created in Email Gateway Defense</b></p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>Your organization creates Sender Policies using <a href="#">Email Gateway Defense</a>.</li> <li>The policy must be created for an admin account or an entire domain.</li> <li>It does not apply to policies created for specific end users.</li> </ul>	<ul style="list-style-type: none"> <li><b>Block sender policy</b> – The policy is to block mail from a sender.</li> <li>Number of emails detected – How many emails are affected by the sender policy.</li> <li>Number of mailboxes affected – How many mailboxes are affected by the sender policy. Note that this number might increase if you are still experiencing a malicious email attack.</li> <li><b>Quarantine sender policy</b> – The policy is to quarantine mail from a sender.</li> <li>Sender country – Where the email originated.</li> <li><b>Policy created by</b> – The creator of a Sender Policy.</li> </ul>	<p>Same as above</p>

<p><b>User-reported email submitted</b></p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• Your organization must be using the <a href="#">Barracuda Outlook add-in</a> for reporting questionable emails.</li> <li>• An end user in your organization must report an email by using the Barracuda Outlook add-in.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Email subject</b> – Subject of the user-reported email.</li> <li>• <b>External/Internal email</b> – Whether the email originated outside of or within your organization.</li> <li>• <b>Number of mailboxes affected</b> – How many mailboxes are affected by the reported email. Note that this number might increase if you are still experiencing a malicious email attack.</li> <li>• <b>Number of users reported</b> – How many users reported this same email. This value equals 1 for the first reporter, then increases by 1 for each user who reports an email with the same sender and subject.</li> <li>• <b>Reported by</b> – User who reported the suspicious email.</li> <li>• <b>Sender country</b> – Where the email originated.</li> <li>• <b>Sender email</b> – Sender of the user-reported email.</li> </ul>	<p>Same as above</p>
<p><i>Additional triggers will be added over time.</i></p>		

Triggers and Actions are required when creating an automated workflow; Conditions are not required. As shown in Figure A below, you can create a workflow that just has a Trigger, like a User-reported email submitted, and an action, like Create Slack notification. So whenever a new user-reported email is submitted – regardless of the subject, sender email, or other values – an alert notification is sent.



You can optionally specify multiple values per component in a single workflow. For example, as shown in Figure B above, you can create a workflow which requires triggers for both the sender email and email subject. Then, you can choose to have both an action to create an incident and another action to send a Slack notification. Figure C shows both multiple conditions and multiple actions.

### Specifying AND vs OR Conditions

When creating workflow with two or more conditions, you might want to specify whether individual conditions can set off an action (OR scenario) or whether a combination of conditions is required (AND scenario) before an action can be taken.

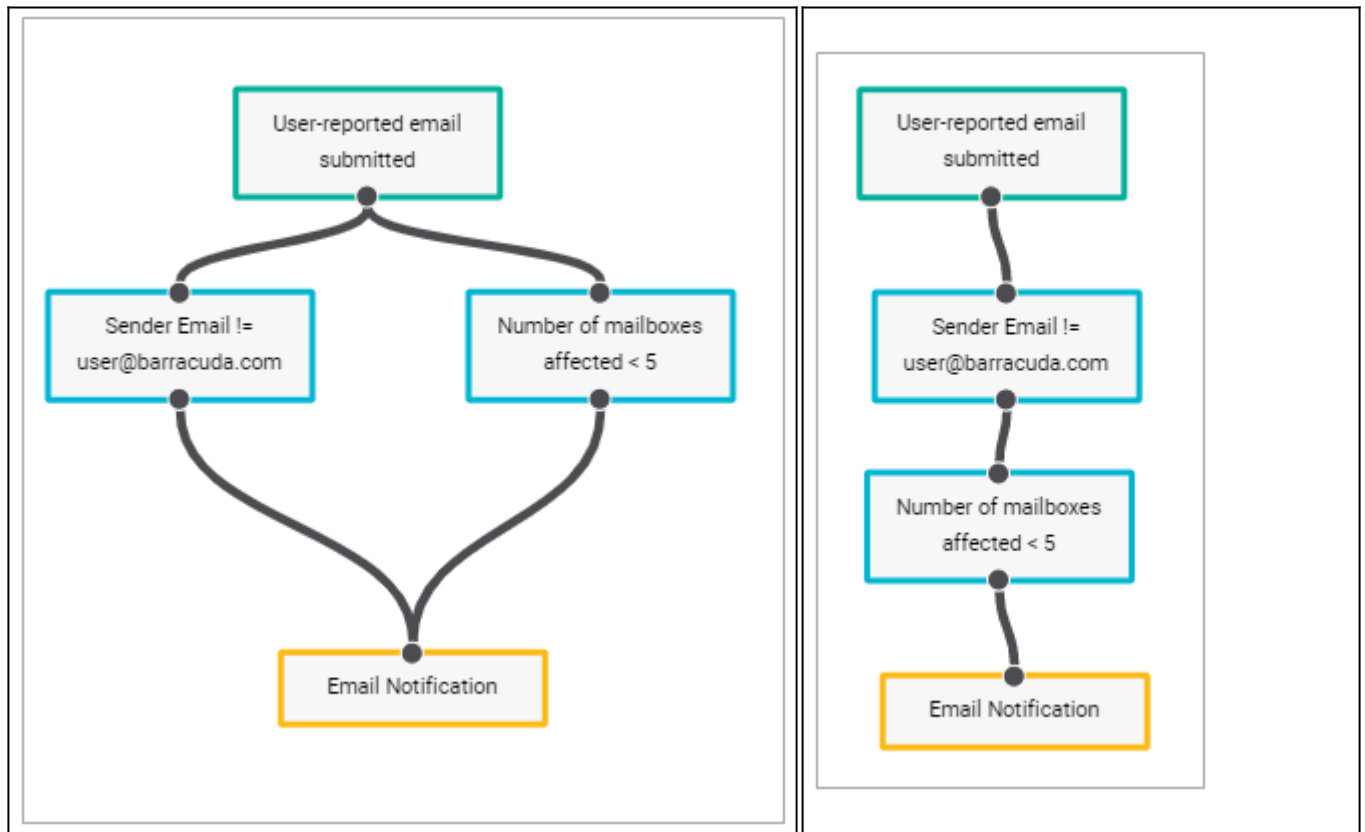
Figure D below shows an OR scenario, where either of the conditions' being met is enough to set the action in motion. You might think of OR scenarios as a parallel flow. When you create workflows, they are created as OR scenarios by default.

Figure E below shows an AND scenario, where both conditions must be met before the action can be taken. You might think of AND scenarios as a serial flow. When you create workflows and want to change from the default OR scenario to an AND scenario, you must rearrange the nodes, delete some of the original connections, and draw new connections. Check that the nodes in your workflow are all connected and will produce your desired effect. If, for example, you have competing conditions, the actions in your workflow will never be taken.

The examples in Figure D and Figure E are relatively simple. You can create much more complex workflows with combinations of AND and OR scenarios.

**Figure D**  
**OR Scenario - Only One Condition Must Be Met**

**Figure E**  
**AND Scenario - Both Conditions Must Be Met**



## Workflow Templates

Rather than creating a completely new automated workflow, you can use workflow templates as a starting point to create workflows for common scenarios. For example, you can use the **User-reported Message - Create Incident - Specific User** template to create a workflow to create an incident whenever a specific user reports a message. When you select the template, the workflow appears automatically. On the left side of the page, you are prompted to complete the condition, in this case, to specify the user who is reporting the message. You can optionally change other parts of the workflow, for example, to change the condition to add another user, to add the number of affected mailboxes, and so on. Be sure to specify a unique name for each workflow you create.

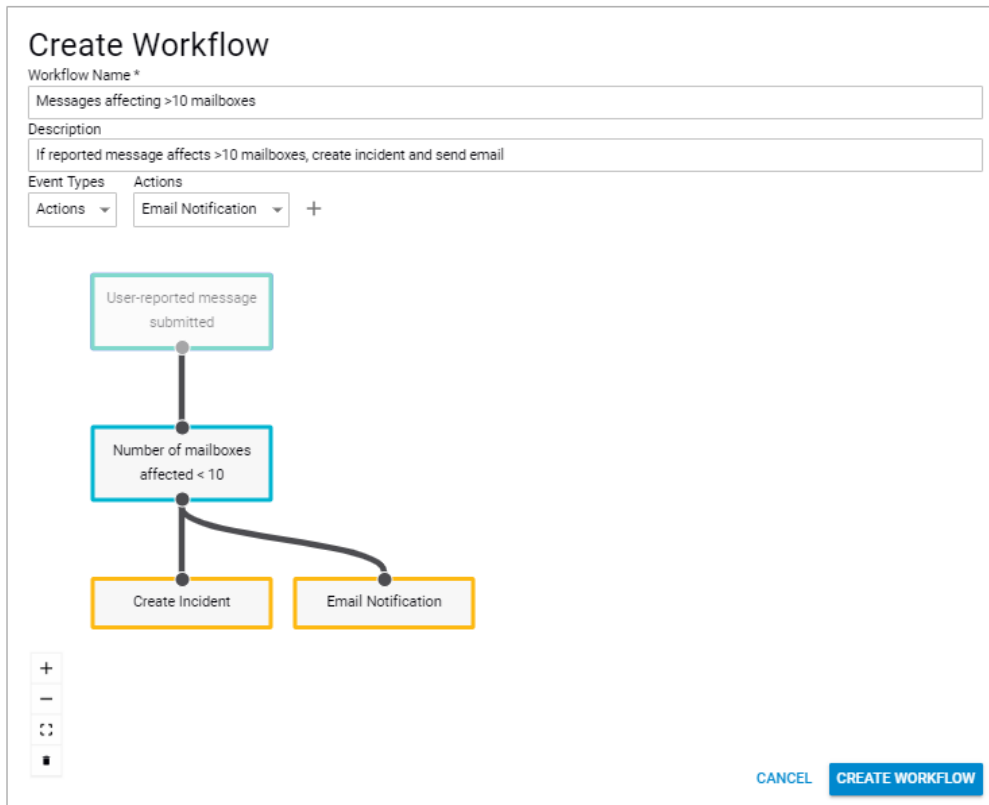
Additional workflow templates will be added over time.

## Creating an Automated Workflow

To create a workflow using a template, refer to the next section, [Creating an Automated Workflow using a Template](#).

To create an automated workflow:

1. Open Incident Response.
2. From the menu in the upper left corner, select **Automated Workflows**.
3. On the **Automated Workflows** page, click **Create Workflow**.
4. Under **Workflow Templates**, select **Blank Template**. To use a specific template, see the following section.
5. Provide a unique name for the workflow.
6. Optional. Provide a description for the workflow.
7. Select a trigger from the **Triggers** list. Click the plus (+) icon. The trigger appears in the graphical workflow space.
8. Optional. In the **Event Types** menu, switch your selection to **Conditions**. Select a condition from the **Conditions** list. Specify an operator (Equals, Does not equal, Greater than, Less than), then specify the value in the **Condition Details** field. Click the plus (+) icon. The condition appears in the graphical workflow space.
9. For example, you might specify that the **Number of mailboxes affected is Greater than 10**. If needed, repeat this step for additional conditions in this workflow.
10. In the **Event Types** menu, switch your selection to **Actions**. Select an action from the **Actions** list. Click the plus (+) icon. The action appears in the graphical workflow space. If needed, repeat this step for additional actions in this workflow.
11. Review the graphical representation of the workflow. Triggers are shown in the top level, followed by Conditions, then Actions on the lowest level.



**Create Workflow**

Workflow Name \*  
Messages affecting >10 mailboxes

Description  
If reported message affects >10 mailboxes, create incident and send email

Event Types: Actions  
Actions: Email Notification +

Workflow Diagram:

```
graph TD; A[User-reported message submitted] --> B[Number of mailboxes affected < 10]; B --> C[Create Incident]; B --> D[Email Notification];
```




+  
-  
↺  
■

CANCEL CREATE WORKFLOW

Take the following actions, if needed:

- **Check connections** – Check that connections exist between the various parts of your

workflow. If your workflow actions are not connected to the rest of your workflow, they can not be taken.

- **Rearrange components** – Click and drag components to new locations.
- **Add components** – Repeat the step above to add one or more new components.
- **Change the value for a condition** – Remove the condition component, then add a new condition component with the desired value.
- **Remove connections** – If you are changing from an OR to an AND scenario, be sure to remove any unneeded connections. Click the connection to select it, then click the trash icon  in the toolbar.
- **Remove a workflow component** – Click the component to select it, then click the trash icon  in the toolbar.  
Note that you cannot delete a trigger if it has associated conditions. Either delete all of the conditions and then delete the trigger, or click **Cancel** and start a new workflow.
- **Zoom in/out/re-center** – Use the +/- icons in the toolbar to zoom in and out on your workflow. To re-center the workflow, click  in the toolbar.

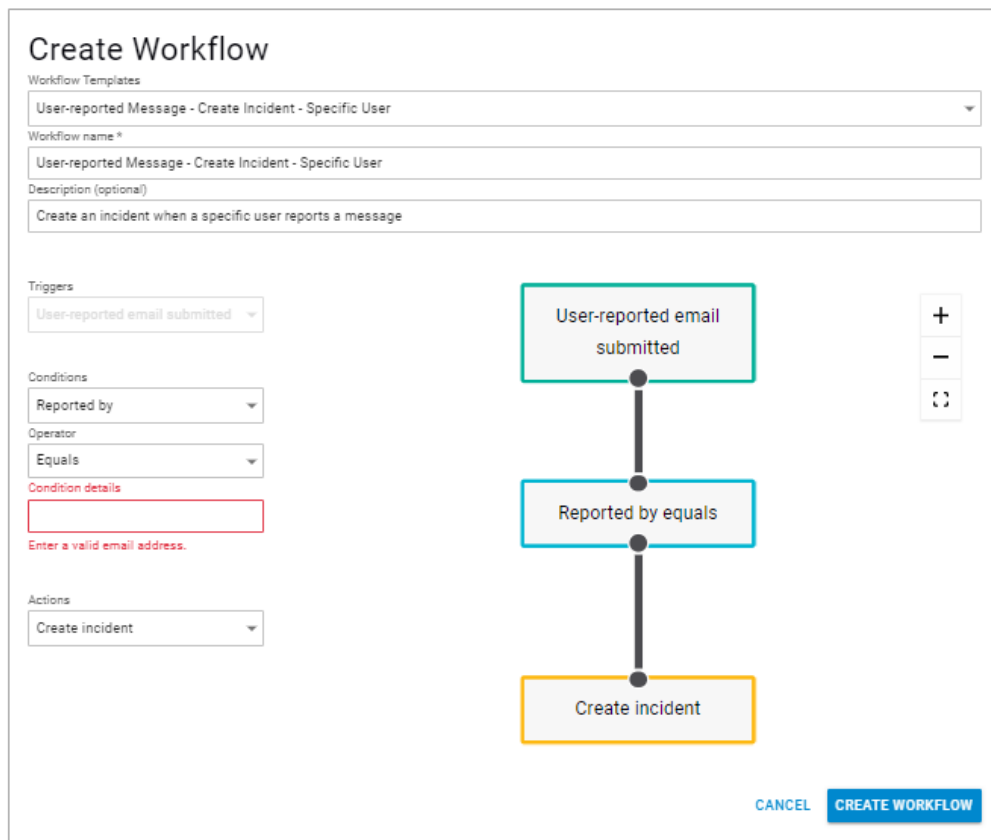
12. Click **Create Workflow**.

13. The workflow appears in table on the **Automated Workflows** page. It is ready to launch whenever it is triggered.

## Creating an Automated Workflow using a Template

To create an automated workflow using a template:

1. Open Incident Response.
2. From the menu in the upper left corner, select **Automated Workflows**.
3. On the **Automated Workflows** page, click **Create Workflow**.
4. Under **Workflow Templates**, a specific template, such as **User-reported Message - Create Incident - Specific User**, to use as the basis for creating a workflow.
5. Provide a unique name for the workflow.
6. Optional. Provide a description for the workflow.
7. On the left side of the page, red text indicates conditions you must enter to customize the template. In this example, provide the email address for the user who is reporting emails. Complete the information. Notice it automatically updates in the workflow.



**Create Workflow**

Workflow Templates  
User-reported Message - Create Incident - Specific User

Workflow name\*  
User-reported Message - Create Incident - Specific User

Description (optional)  
Create an incident when a specific user reports a message

Triggers  
User-reported email submitted

Conditions  
Reported by  
Operator  
Equals  
Condition details  
Enter a valid email address.

Actions  
Create incident

Graphical representation of the workflow:

```
graph TD; A[User-reported email submitted] --> B[Reported by equals]; B --> C[Create incident];
```

CANCEL CREATE WORKFLOW

8. Optionally add more conditions or actions, as described in the section above.
9. Review the graphical representation of the workflow. If needed, take actions as described in the section above.
10. Click **Create Workflow**.
11. The workflow appears in table on the **Automated Workflows** page. It is ready to launch whenever it is triggered.

## Reviewing and Taking Action with Automated Workflows


To review and take action on automated workflows:


1. Open Incident Response.
2. From the menu in the upper left corner, select **Automated Workflows**.  
The **Automated Workflows** table displays all automated workflows created for your account. For each automated workflow, you can view the following information:
  - Created on – Date the admin created the workflow.
  - Workflow Name – Name given to the workflow by the creator.
  - Edited By – The last person to edit the workflow.
  - Times Triggered – How many occurrences of the trigger event have occurred.
  - Conditions Checked – How many times the conditions in the workflow were checked. In a workflow like that shown in Figure B above, where the number of conditions and triggers are equal, the Conditions Checked value equals the Times Triggered value. In a workflow

like that shown in Figure C above, there are twice as many conditions as triggers, so the Conditions Checked value should be twice that of the Times Triggered value.

- Actions Taken – How many times the action(s) for this workflow have been completed. In a workflow like that shown in Figure A above, where the number of triggers and actions are equal, the Actions Taken value equals the Times Triggered value. In a workflow like that shown in Figure B above, there are twice as many actions as triggers, so the Actions Taken value should be twice that of the Times Triggered value.


**To edit a workflow**, click the pencil  icon in the **Actions** column.

**To disable a workflow**, click the pause  icon in the **Actions** column. The workflow disappears from the Automated Workflows table and is available when you click **Show Disabled**.

**To view details about the workflow**, click the clipboard  icon in the **Actions** column.



### Viewing and Reactivating Disabled Automated Workflows

To view disabled workflows, click **Show Disabled**. You can edit workflows in the disabled state.

To re-enable a workflow on this list, click the play  icon in the Actions column. Click **Show Enabled** to view it.

### Viewing Incidents Created by Automated Workflows

To view an Incident from within Automated Workflows:

1. in the **Automated Workflows** table, locate the workflow that created the incident you want to see. Click **View Workflow** .  
The **View Workflow** page displays.
2. In the **Automated Workflow Runs** table, click the plus icon  next to the run of this workflow you want to investigate.
3. In the **Event Result** column, click **Incident created**.  
The View Incident page displays. There you can view the details of the incident. Click the **Automated Workflow** link to return to the **View Workflow** page.

### Viewing an Incident from the Incidents Page

Incidents created by automated workflows are listed on the **Incidents** page, along with all other incidents, and are shown as being created by an automated workflow. When you view the incident details, click the **Automated Workflow** link to see the workflow that initiated the incident. For more information on viewing incidents, refer to [Reviewing Incidents](#).

## Figures

1. workflow.png
2. noConditions2.png
3. multipleActions2.png
4. multipleActions2x2.png
5. OR.png
6. AND.png
7. workflow.plain.png
8. AWdelete.png
9. AWdelete.png
10. AWcenter.png
11. workflowTemplates.png
12. pencil.png
13. pause.png
14. clipboard.png
15. play.png
16. viewWorkflow.png
17. plusIcon.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.