

# EIM Policy Elements

- EN
- FR

This topic lists the different elements that you can use in EIM policy documents.



EIM policies are case sensitive. All elements must start with an upper-case letter.

## Related Pages

- [EIM Policy Grammar](#)
- [Resource Identifiers](#)

Element	Required	Description	Examples
Statement	Yes	<p>The <code>Statement</code> element is the main one, and is required in every <code>policy-document</code> attribute.</p> <p>There is one <code>Statement</code> element per policy document that contains an array of one or more individual statements, corresponding to JSON blocks enclosed in braces <code>{}</code> and that contain at least an <code>Action</code> or <code>NotAction</code>, <code>Effect</code> and <code>Resource</code> or <code>NotResource</code> elements.</p> <div data-bbox="389 861 711 966"><p> The order of these elements within the individual statement is not important.</p></div>	<pre>"Statement": [   {     "Action":     [ "..."],     "Effect": "...",     "Resource":     [ "..."]   },   {     "Action":     [ "..."],     "Effect": "...",     "Resource":     [ "..."],     "Sid": "...",   } ]</pre>
Sid	No	<p>The <code>Sid</code> (statement ID) element is an optional ID that you can add to individual statements. This enables you to give them a name according to your needs, but is not used by EIM to identify them.</p>	<pre>"Sid": "Admin1"</pre>

Action	No	<p>The <code>Action</code> element specifies one or more actions that are allowed or denied. Every individual statement requires either the <code>Action</code> or the <code>NotAction</code> element.</p> <p>To specify an action, you must specify the service followed by a colon, and use the name of an API method (for example <code>DescribeInstances</code>). For more information, see <a href="http://docs.outscale.com/">http://docs.outscale.com/</a>.</p> <p>You must use one of the following codes:</p> <ul style="list-style-type: none"> <li>For the OUTSCALE API: <code>api</code></li> <li>For Flexible Compute Unit (FCU): <code>ec2</code></li> <li>For Load Balancing Unit (LBU): <code>elasticloadbalancing</code></li> <li>For Elastic Identity Management (EIM): <code>iam</code></li> <li>For DirectLink: <code>directconnect</code></li> <li>For all the services above: <code>*</code></li> </ul> <div data-bbox="386 680 711 764" style="border: 1px solid orange; padding: 5px; margin: 10px 0;">  Action names are case sensitive. </div> <p>The <code>Action</code> element is an array that contains one or more actions, enclosed in quotation marks and separated by commas.</p> <p>You can use wildcards to replace parts of action names and thus specify several actions at the same time. You can for example specify all actions in all services or all actions in a specified service. You can also use wildcards to specify all actions regarding the same object type.</p>	<ul style="list-style-type: none"> <li>Action element specifying two actions: <div data-bbox="776 218 1068 344" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"Action": [ "ec2:DescribeInstances", "ec2:RunInstances" ]</pre> </div> </li> <li>Action element specifying all actions in all services: <div data-bbox="776 428 1068 499" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"Action": [ "*" ]</pre> </div> </li> <li>Action element specifying all actions in EIM: <div data-bbox="776 583 1068 655" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"Action": [ "iam:*" ]</pre> </div> </li> <li>Action element specifying all actions regarding volumes, that is actions that include the <code>Volume</code> string (<code>AttachVolume</code>, <code>CreateVolume</code>, <code>DeleteVolumes</code>, <code>DescribeVolumes</code>, <code>DeleteVolume</code>): <div data-bbox="776 823 1068 928" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"Action": [ "ec2:*Volume*" ]</pre> </div> </li> </ul>
NotAction	No	<p>The <code>NotAction</code> element specifies one or more exceptions to a list of actions. Every individual statement requires either the <code>Action</code> or the <code>NotAction</code> element.</p> <p>The <code>NotAction</code> element format is the same as the <code>Action</code> element one.</p> <p>You can use the <code>NotAction</code> element to create shorter statements instead of specifying a long list of actions in the <code>Action</code> element. You can for example allow all actions using the <code>Action</code> element, except one or more actions that you specify in the <code>NotAction</code> element. As you need to explicitly allow actions, only specifying an action in the <code>NotAction</code> element alongside and allow does not grant permissions to all other actions.</p>	<p><code>NotAction</code> element that excludes the <code>DescribeInstances</code> action from the permissions:</p> <div data-bbox="732 1199 1068 1297" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"NotAction": [ "ec2:DescribeInstances" ]</pre> </div> <ul style="list-style-type: none"> <li>If this element is associated with <code>Effect="Deny"</code> and a <code>Action="["*"]</code>, all other actions than <code>DescribeInstances</code> are explicitly denied.</li> <li>If this element is associated with <code>Effect="Allow"</code> and <code>Action="["*"]</code>, all actions are allowed except <code>DescribeInstances</code>.</li> </ul>
Effect	Yes	<p>The <code>Effect</code> element specifies whether the statement explicitly allows or denies actions.</p> <p>Valid values for the <code>Effect</code> element are either <code>Allow</code> or <code>Deny</code>.</p> <p>By default, access to resources is denied until it is explicitly allowed in a policy statement. To enable users to access resources, you must set the <code>Effect</code> element to <code>Allow</code>. Setting the <code>Effect</code> element to <code>Deny</code> overrides any allow that may be set in another statement.*</p>	<div data-bbox="732 1703 1068 1774" style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <pre>"Effect": "Allow"</pre> </div>

Resource	No	<p>The <code>Resource</code> element specifies the resources covered by the statement. Every individual statement requires either the <code>Resource</code> or the <code>NotResource</code> element.</p> <p>The <code>Resource</code> element contains an array of one or more resource specifications, enclosed in quotation marks and separated by commas.</p> <p>You must use the OUTSCALE Resource Name format to specify the resources. You can specify individual resources, or use wildcards to specify a resource type, resources of a service or all resources. For more information, see <a href="#">EIM Policy Elements</a>.</p>	<ul style="list-style-type: none"> <li>Resource element specifying an individual security group and an individual instance: <pre>"Resource": [ "arn:aws:ec2:eu-west-2:123456789000:security-group/sg-abcd1234", "arn:aws:ec2:eu-west-2:123456789000:instance/i-abcd1234" ]</pre> </li> <li>Resource element specifying all resources in all services: <pre>"Resource": [ "*" ]</pre> </li> <li>Resource element specifying all FCU instances in eu-west-2 Region: <pre>"Resource": [ "arn:aws:ec2:eu-west-2:123456789000:instance/*" ]</pre> </li> <li>Resource element specifying all FCU and LBU resources: <pre>"Resource": [ "arn:aws:ec2:*", "arn:aws:elasticloadbalancing:*" ]</pre> </li> </ul>
NotResource	No	<p>The <code>NotResource</code> element specifies one or more exceptions to a list of resources. Every individual statement requires either the <code>Resource</code> or the <code>NotResource</code> element.</p> <p>The <code>NotResource</code> element format is the same as the <code>Resource</code> one.</p> <p>You can use the <code>NotResource</code> element to create shorter statements instead of specifying a long list of resources in the <code>Resource</code> element. You can for example allow actions on all resources using the <code>Resource</code> element, except on one or more resources that you specify in the <code>NotResource</code> element.</p>	<p><code>NotResource</code> element that excludes a security group from the list of resources:</p> <pre>"NotResource": [ "arn:aws:ec2:eu-west-2:123456789000:security-group/sg-abcd1234" ]</pre> <p>If this element is associated with <code>"Effect":Allow</code> and <code>"Resources"="arn:aws:ec2:eu-west-2:123456789000:security-group/*"</code>, all listed actions in the <code>Action</code> element are allowed on all your security group except the one specified above.</p>

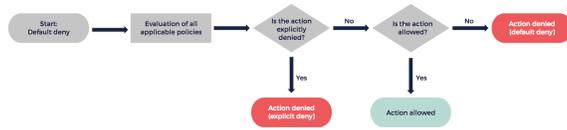
**\*EIM policy evaluation logic and the difference between default and explicit deny:**

When a user sends a request, EIM evaluates this request in regards of all applicable inline or managed policies.

If you did not explicitly allow the action contained in the request in a policy statement for this user, the action is denied. This is default deny. However, if you explicitly denied the actions in a policy statement for this user, this action is denied even though another policy statement allows it. This is explicit deny.

In other words, an allow can overrides a default deny, while an explicit deny overrides all allows and cannot be overridden.

The following flow chart shows the process to determine whether the action contained in a request is allowed or denied:



*EIM Policy Evaluation Logic*

**AWS™** and **Amazon Web Services™** are trademarks of Amazon Technologies, Inc or its affiliates in the United States and/or other countries.