

# Account template creation - Permissions

Using Permissions, you can configure what the end users can and cannot do in their accounts.

Sandbox Studio uses IAM Identity Center Permissions Sets for permissions. You can see more details explaining each of the sections of this page at <https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetcustom.html>

## Default permissions

By default, "Administrator Access" is provided to end users.


Service Control Policies (SCP) are still applied on the accounts and even with Administrator access, some resources and actions may be blocked by your Administrators.

If the default configuration suits your needs, proceed to the next step [Account template creation - Roles & Access](#)

## Customise permissions

For more granular permissions configuration, you can customise the permissions you provide to the end users by selecting **No, I want to customise permissions:**

### Default Permissions

 You can restrict which AWS services and actions are allowed for users using this account template. The default is **Administrator Access** which means full access.

**Use default settings?**

Yes, use default permissions

No, I want to customise permissions

The following sections can be configured:

**Account Permissions**  
What permissions should be applied to this account template?

**AWS Managed Policies \*** 1  
[What are AWS Managed Policies?](#)

Administrator Access X

Include Customer Managed Policies 2

Include Inline Policy 3

## 1. AWS Managed Policies

By default, the Administrator Access policy is applied but you can select one or more policies from the list of AWS Managed policies. More details here about AWS Managed policies:

<https://docs.aws.amazon.com/aws-managed-policy/latest/reference/about-managed-policy-reference.html>

**AWS Managed Policies \***  
[What are AWS Managed Policies?](#)

Amazon Bedrock Full Access X Amazon Sage Maker Full Access X

Q Sage Maker|

- Amazon Sage Maker Read Only
- Amazon Sage Maker Full Access
- AWS Application Autoscaling Sage Maker Endpoint Policy
- AWS Glue Console Sage Maker Notebook Full Access
- Amazon Sage Maker Notebooks Service Role Policy
- Amazon Sage Maker Mechanical Turk Access

## 2. Customer Managed Policies

If you have pre-defined policies you manage, you can use them here. [More details about Customer managed policies](#)

### Customer Managed Policies \*

[What are Customer Managed Policies?](#)

MyCustomPolicyForFullS3Access X

Q Search...

- XRayAccessPolicy-eb2d080e-aa50-4fe0-8688-d2e9388d5738
- MyCustomPolicyForFullS3Access
- SESSCrossAccountPolicy
- XRayAccessPolicy-2e2ea83c-4f67-4423-a65b-d6104d0af979
- SendMail

## 3. Inline policy

Finally, you can use inline policy (define the access directly in the section). [More details about inline policies.](#)

Example:

## Inline Policy \*

[What are Inline Policies?](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "ec2:RunInstances",
8         "ec2:StartInstances",
9         "ec2:StopInstances",
10        "ec2:RebootInstances",
11        "ec2:TerminateInstances",
12        "ec2:CreateTags"
13      ],
14      "Resource": "*"
15    }
16  ]
17 }
```

## Permission Boundary:

Finally, and following the same principles as previous options, you have the option to include **Permission boundaries**. [More details about Permission boundaries.](#)

### Permission Boundary

Advanced settings to restrict permissions

Include Permission Boundary

#### Permission Boundary \*

What type of permission boundary do you want to use?

- AWS managed policy
- Customer managed policy

#### AWS Managed Policy \*

Select an AWS managed policy to use as a permission boundary

Amazon EC2 Read Only Access X

Note: Permission boundaries can only be "AWS managed policy" OR "Customer managed policy" (Not both). In addition, you can only select **ONE** policy to apply.

Having completed all the fields on the **Permissions** page as needed, click on **Next** to move to [Account template creation - Roles & Access](#)

## Example:

This example restricts users to only basic EC2 actions:

## Use default settings?

- Yes, use default permissions
- No, I want to customise permissions

## Account Permissions

What permissions should be applied to this account template?

### AWS Managed Policies \*

[What are AWS Managed Policies?](#)

Amazon EC2 Read Only Access X

Include Customer Managed Policies

Include Inline Policy

### Inline Policy \*

[What are Inline Policies?](#)

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": [
7          "ec2:RunInstances",
8          "ec2:StartInstances",
9          "ec2:StopInstances",
10         "ec2:RebootInstances",
11         "ec2:TerminateInstances",
12         "ec2:CreateTags"
13       ],
14       "Resource": "*"
15     }
16   ]
17 }
```

Revision #7

Created 2025-07-22 18:16:13 UTC by Winston

Updated 2026-04-03 22:39:26 UTC by Paul