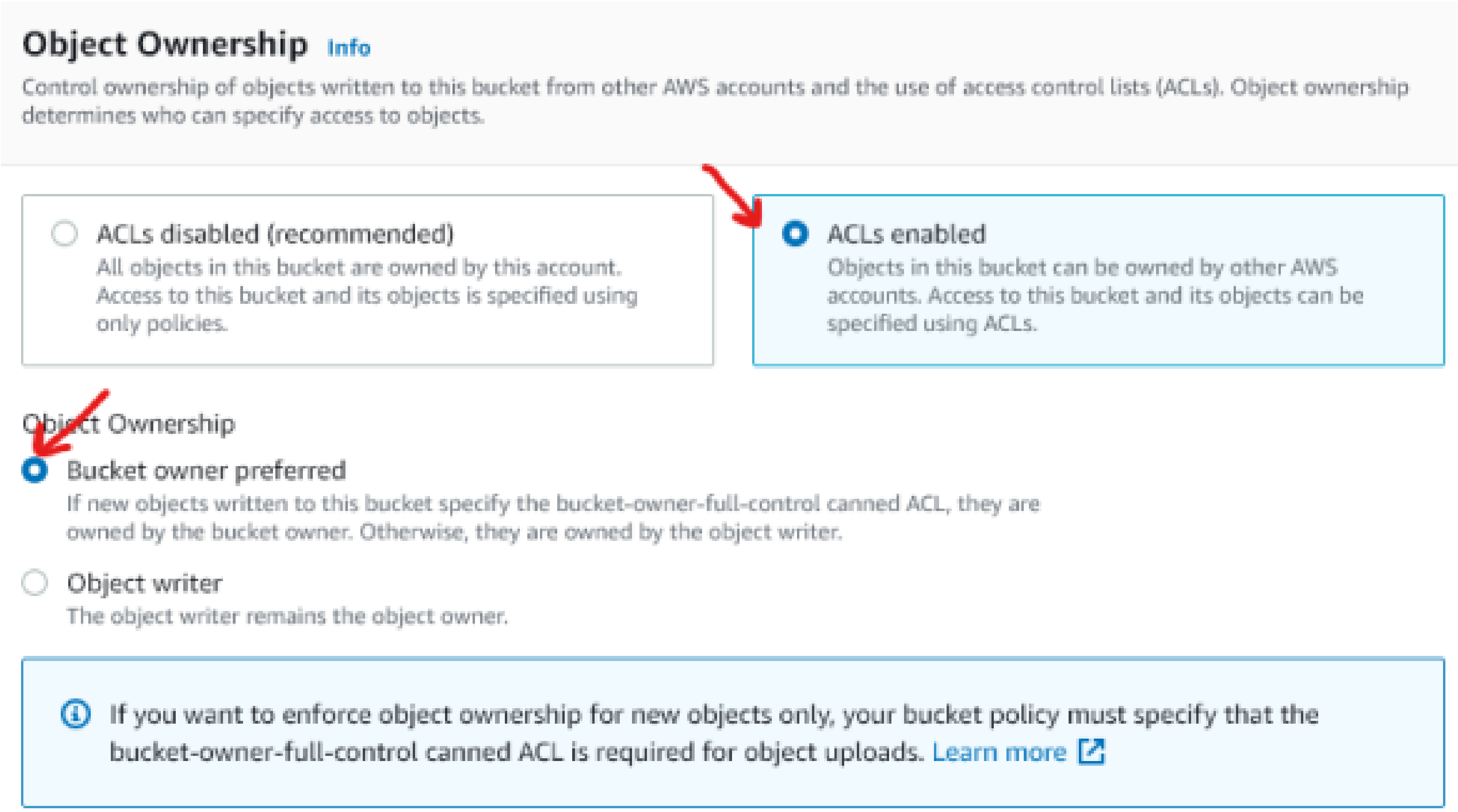
Amazon Web Services (AWS)

Bucket Creation Update

This document is a guide for the updated AWS UI. It will cover how to find the settings shown in the video and, if relevant, the updated settings to use. If it isn't mentioned it has not changed.

Create bucket

When creating a bucket, there are a few new configuration options than shown in the video. Most of them can be left default, but the **Object Ownership** setting (below) needs to be set as shown with the **ACLs enabled** option checked.



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

Bucket settings

The S3 Bucket options page is now a scrollable page broken into sections - all the settings shown in the video are still available. The changes are covered below in the order of the video.

On the **properties** tab **static website hosting** can now be found, by scrolling down to the bottom. On the **permissions** tab the three settings covered in the video have their own section.

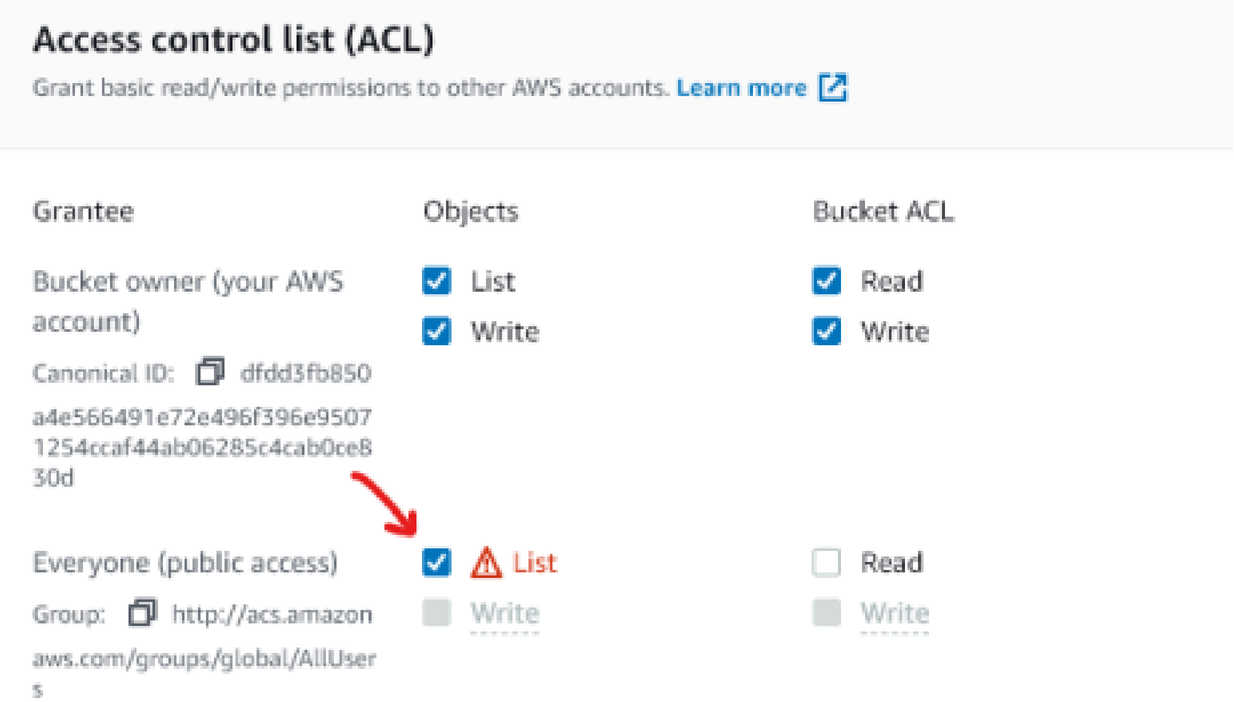
AWS has changed the format of their **CORS** configuration - the updated code is shown below. Paste that into the **Cross-origin resource sharing (CORS)** section.

```
[
    {
        "AllowedHeaders": [
            "Authorization"
        ],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }

  ]
```

The **Bucket Policy** is unchanged.

For the **Access control list (ACL)** section, click edit and enable **List** for **Everyone (public access)** and accept the warning box. If the edit button is disabled, you need to change the **Object Ownership** section above to **ACLs enabled** (refer to Create Bucket section above).



Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: dfdd3fb850a4e566491e72e496f396e95071254ccaf44ab06285c4cab0ce830d	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ List □ Write	□ Read □ Write

Identify and Access Management (IAM)

- Create group

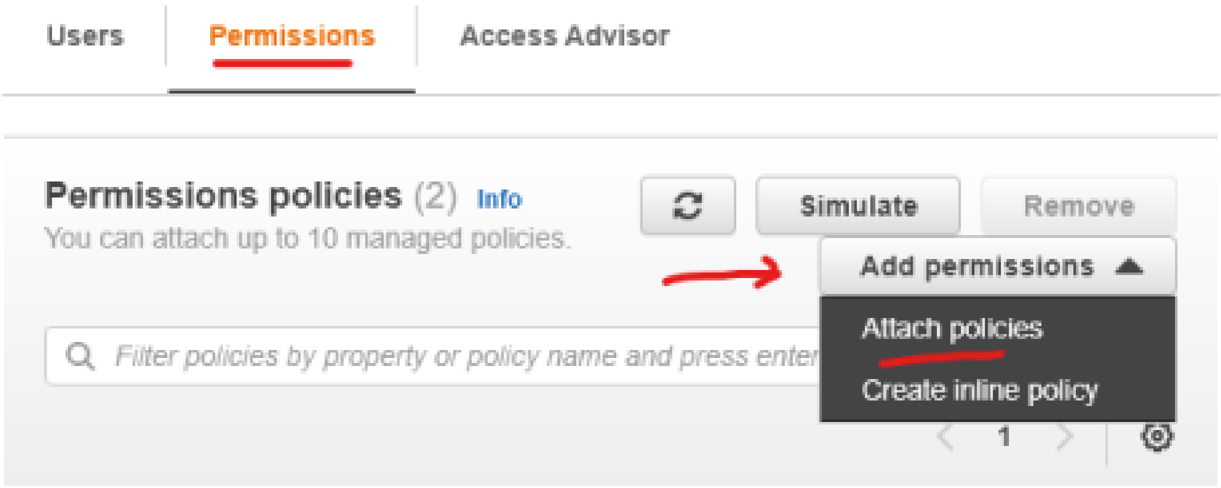
The sidebar name is now **User Groups,** and everything happens on a single page instead of clicking next, as shown in the videos.

- Create policy

On the create policy page, there is now a button to go to the next page to add tags. Tags are optional, but you must click it to get to the **review policy** page.

- Attach policy

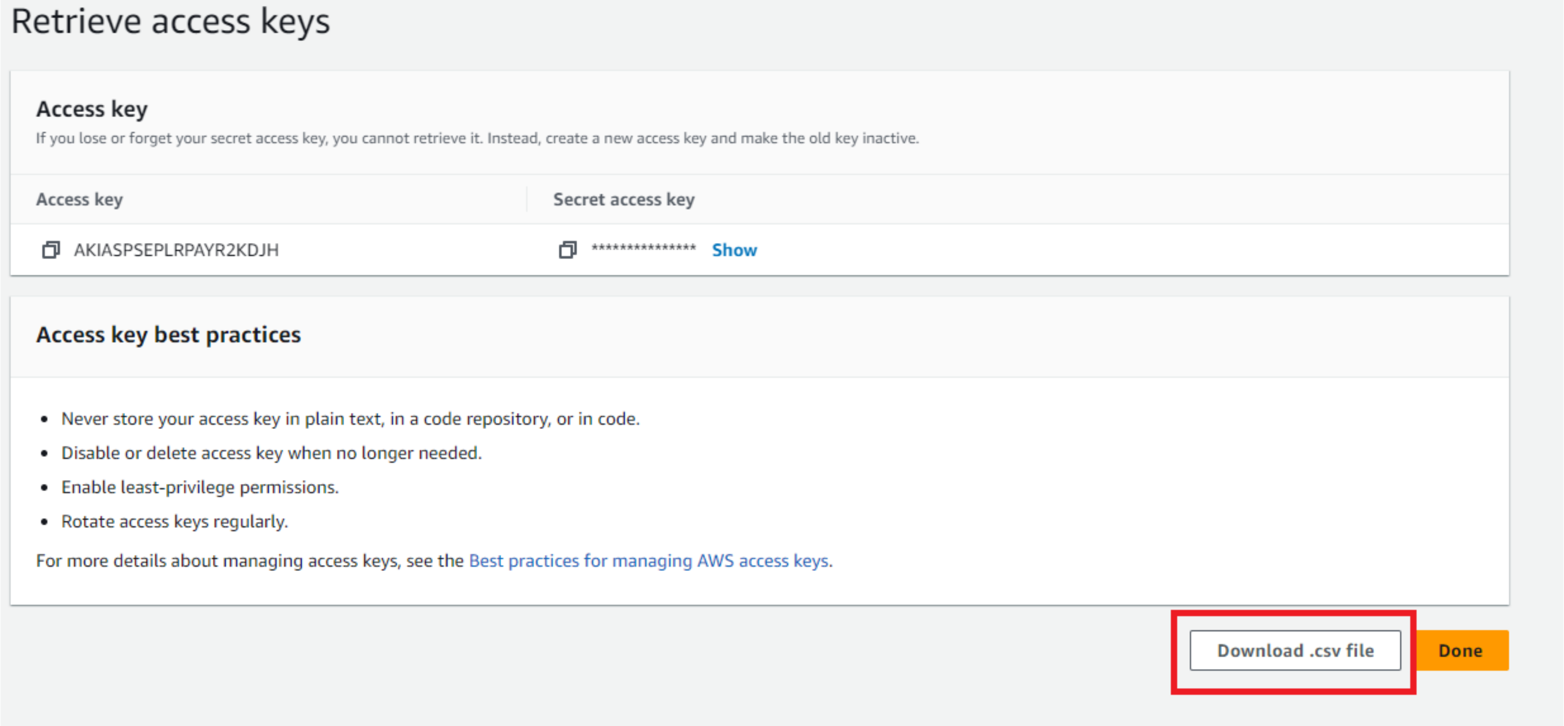
To attach the policy, on the sidebar, click **User Groups.** Select your group, go to the **permissions** tab, open the **Add permissions** dropdown, and click **Attach policies.** Select the policy and click **Add permissions** at the bottom.


Users
Permissions
Access Advisor
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Attach policies
Create inline policy
Filter policies by property or policy name and press enter
1

Retrieve access keys

AWS changed the site layout recently, so the steps to get the CSV file are slightly different.

1. Please follow the steps below to get the CSV file.
2. Go to IAM and select 'Users'
3. Select the user for whom you wish to create a CSV file.
4. Select the 'Security Credentials' tab
5. Scroll to 'Access Keys' and click 'Create access key'
6. Select 'Application running outside AWS', and click next
7. On the next screen, you can leave the 'Description tag value' blank. Click 'Create Access Key'
8. Click the 'Download .csv file' button



Retrieve access keys

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIASPSEPLRPAYR2KDJH	*************** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the Best practices for managing AWS access keys.