## Overview:

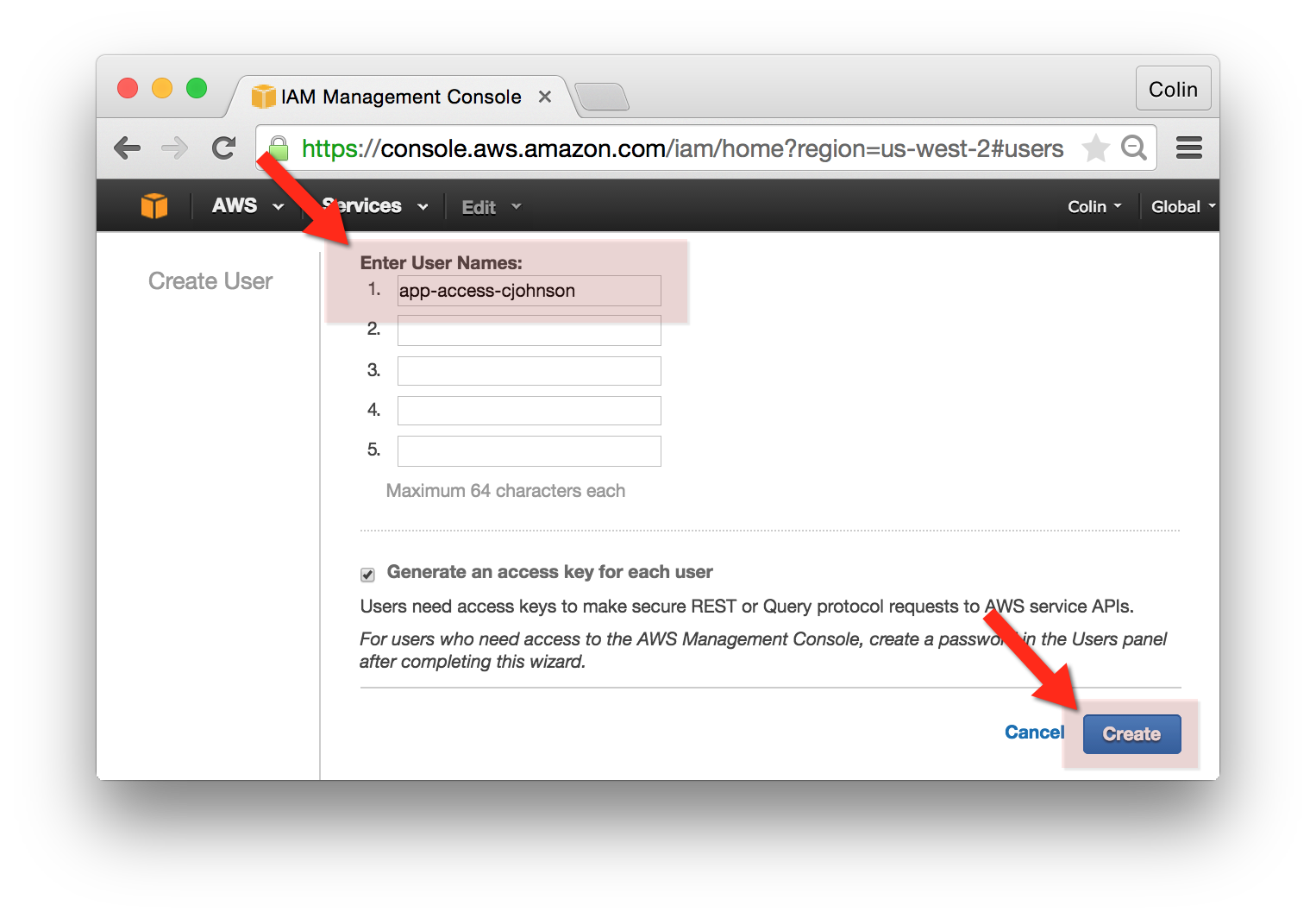
We’ll be creating an IAM user that has access only limited access to an S3 bucket. This use case is fairly common – this is one common method for an application to use an AWS resource. Limiting access is particularly valuable – a misconfigured application could potential read/write/delete data from another environment or application. Limiting access using IAM is one method of ensuring an application accesses only the data it should be accessing.

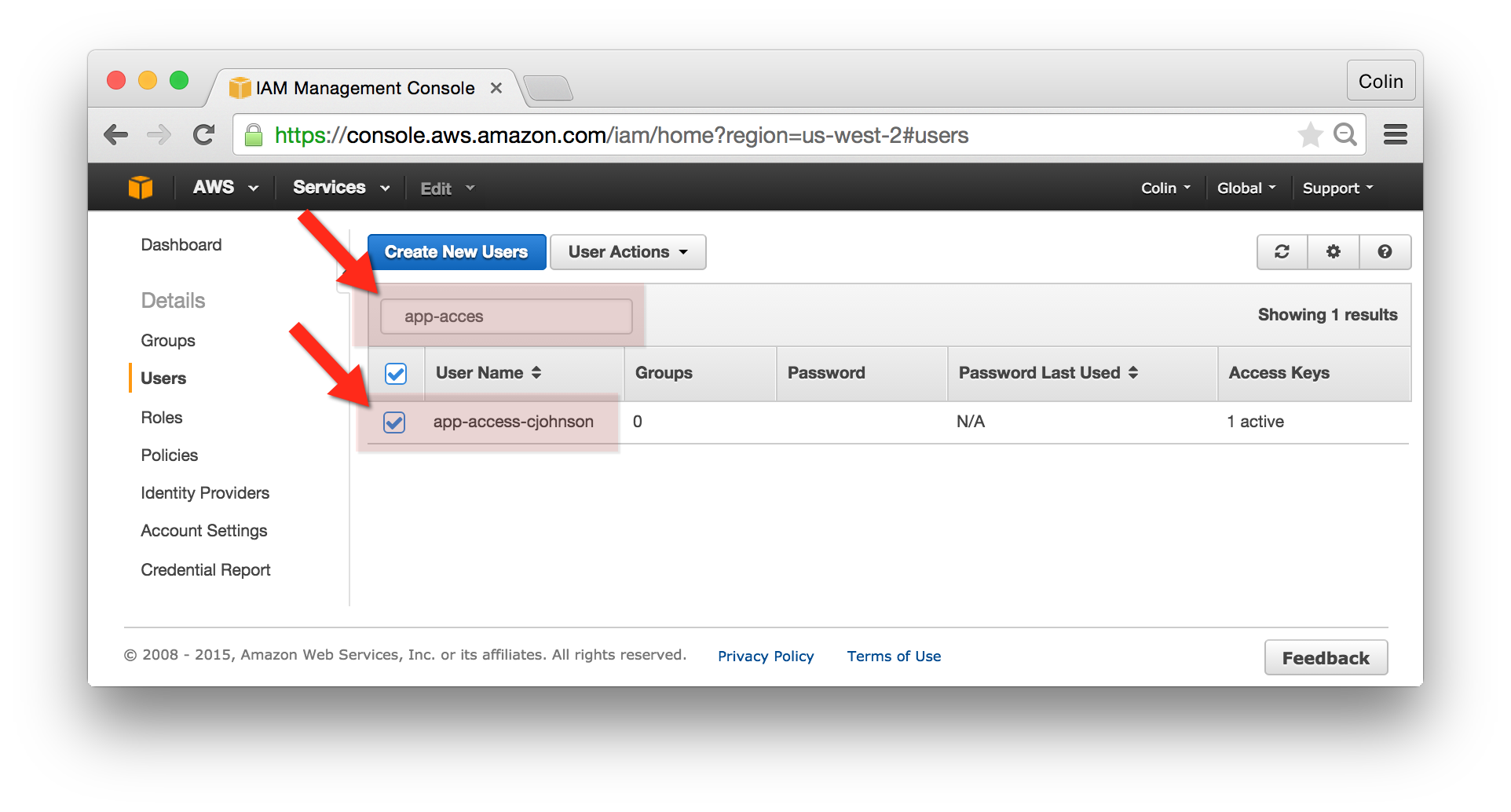
## Create an S3 Bucket in the us-west-2 (Oregon) Region:

1. Go to the AWS S3 Console
2. Click “Create Bucket”
   1. Bucket Name: app-access-yourname
   2. Region: Oregon
   3. Click Create

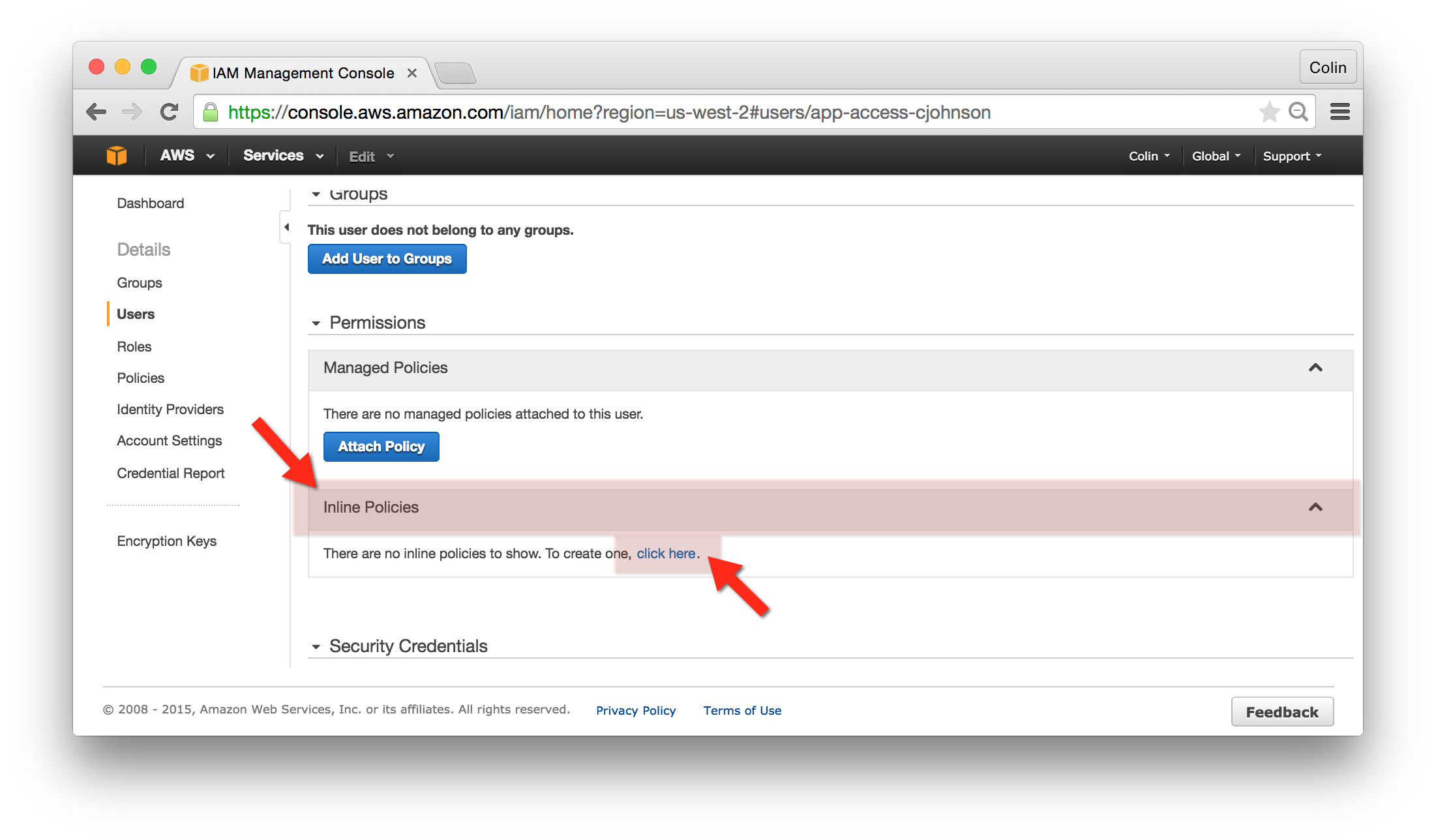
## Create a new IAM User:

1. Go to the AWS IAM Console and select “Users” from the left-hand navigation tab.
2. Click “Create New Users”
   1. Enter User Names: app-access-yourname
   2. Generate an access key for each user: unchecked

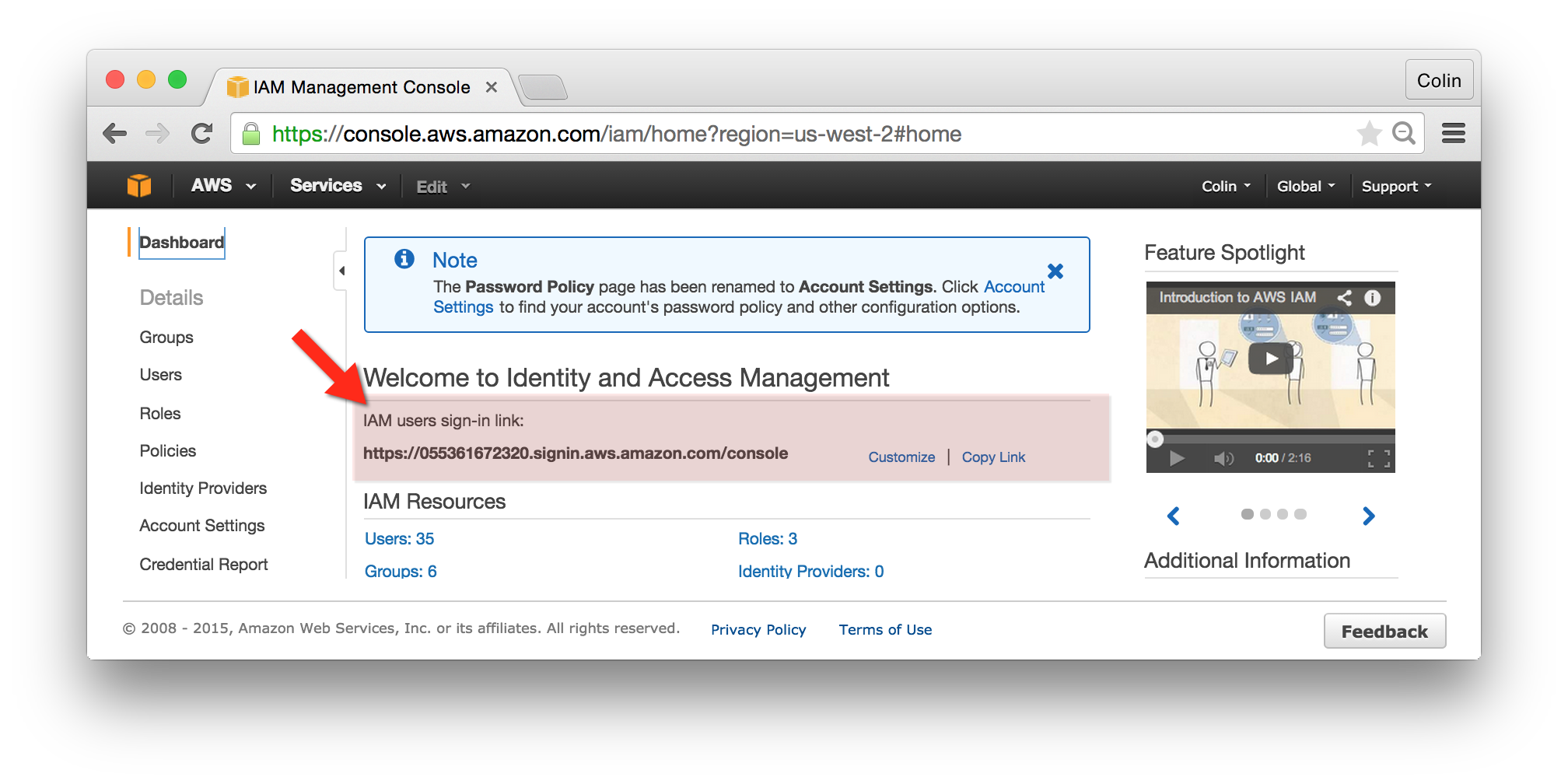


1. In the AWS IAM Console, select “Users” and search for the user app-access-yourname – click on this user.
2. Click the “Manage Password” button.
   1. Select “Assign an auto-generated password”
   2. Click “Apply”
3. Click “Show User Security Credentials”
   1. Make a note of your newly created user’s password.
   2. Click “Close”

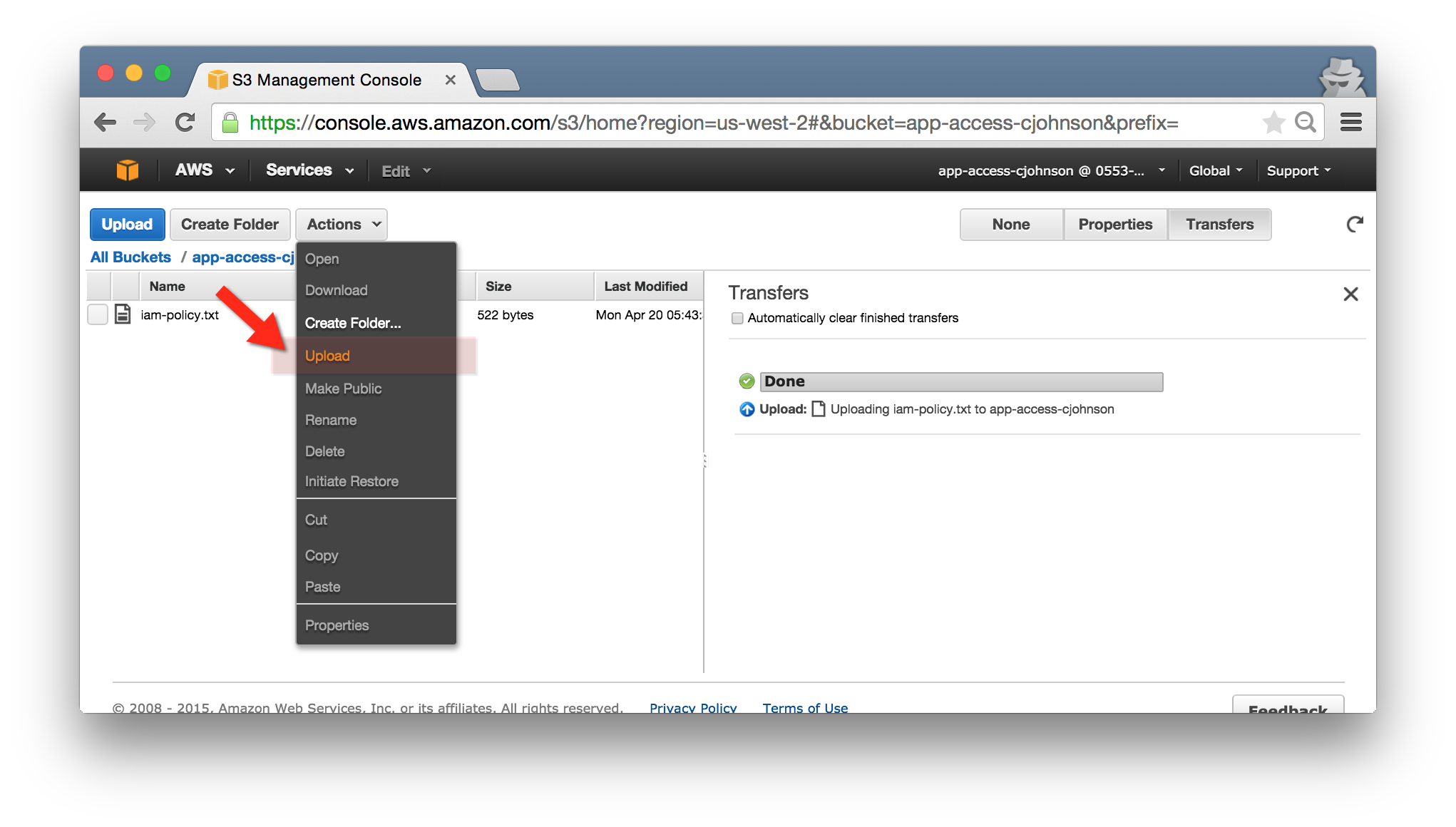
## Allow Limited S3 Access to Your New User:

1. In the AWS IAM Console, select “Users” and search for the user app-access-yourname – click on your new user.
2. Click the arrow next to “Inline Policies” and “click here”  
   
3. Click “Custom Policy” to create a policy:
   1. In the same directory as this file you should see an “app-access-policy.txt” file – open this document and paste the content as the Custom Policy.
   2. Click “Apply Policy”

## Login to the AWS Console with your new user:

1. To get the address of the AWS Console, go to the AWS IAM Console and click “Dashboard” from the left-hand navigation.
2. Locate the “IAM users sign-in link” – it will look similar to <https://055361672320.signin.aws.amazon.com/console>  
   
3. Open a new, private browser window and go to the “IAM User Sign In”

## Upload an Object to the app-access-yourname Bucket:

1. In the new window, go to the AWS S3 Console.
2. Click on the “app-access-youname” Bucket
3. From the “Actions” menu, select “Upload”
   1. Drag and Drop a file to upload a file to this bucket.
4. Next, return to the AWS S3 Console and click on an S3 bucket – you should see the text “Sorry! You do not have permissions to view this bucket”