Lab is ready.
Open the console to begin. Keep the default region.
Tip: open the console in a new window to see it side-by-side with these instructions.

Lab 3: Configure a Web Application to use an Amazon S3 Bucket and Amazon DynamoDB Table

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at *AWS Training and Certification*.

Objectives

After completing this lab, you will be able to:

- Create an Amazon Simple Storage Service (Amazon S3) Bucket
- Create an S3 bucket policy
- Modify an Application to Use an S3 Bucket
- Upload an Object to an S3 Bucket
- Create an Amazon DynamoDB table
- Test an Application Using an Application Web Interface
- Manage Existing DynamoDB Items Using the AWS Management Console
- Create Items in a DynamoDB Table Using the AWS Management Console

PREREQUISITES

This lab requires:

- Notebook computer with Wi-Fi and Microsoft Windows, macOS, or Linux (Ubuntu, SuSE, or Red Hat)
- Administrator access (Microsoft Windows users)
- Internet browser, such as Chrome, Firefox, or Internet Explorer 9 or later

Note: Tablet devices cannot access the lab environment, although they can display student guides.

DURATION

This lab requires 45 minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

- **Expected output:** A sample output that you can use to verify the output of a command or edited file.
- **Note:** A note, tip, or important guidance.
- **Additional information:** Where to find more information.
- **Consider:** A moment to pause to consider how you might apply a concept in your own environment or to initiate a conversation about the topic at hand.
- **Copy/Paste:** A code block that displays the contents of a script or file you need to copy and paste that has been pre-created for you. When you need to copy only a certain part of a code block, there are numbered *TODO* comments in the code.

SCENARIO

Your employee directory application launched successfully, but now you must customize the application to include employee images and information using Amazon S3 and Amazon DynamoDB. In this lab, you create an Amazon S3 bucket and modify the bucket policy. Then, you upload objects (images) to the S3 bucket. Next, you configure the employee directory application to use the S3 Bucket as a data source. Next, you will remove objects from the S3 bucket and test the impact on the application. After configuring the applciation to use Amazon S3, you create an Amazon DynamoDB table. Finally, you use the application interface and DynamoDB to create items in your table and test the functionality of the application.

Start lab

1. To launch the lab, at the top of the page, choose **Start lab**.

You must wait for the provisioned AWS services to be ready before you can continue.

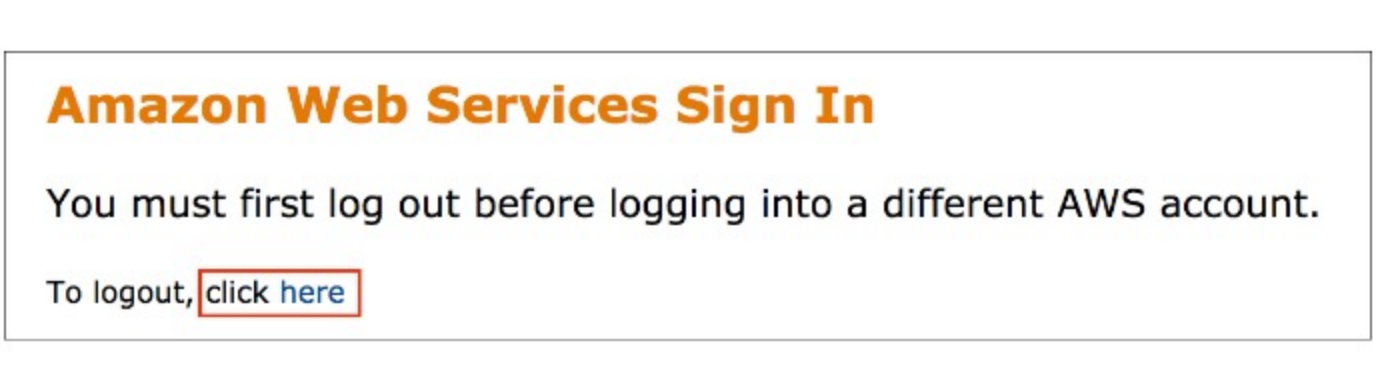
2. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

Do not change the Region unless instructed.

COMMON SIGN-IN ERRORS

Error: You must first sign out



If you see the message, **You must first log out before logging into a different AWS account:**

- Choose the **click here** link.
- Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
- Choose **Open Console** again.

Error: Choosing Start Lab has no effect

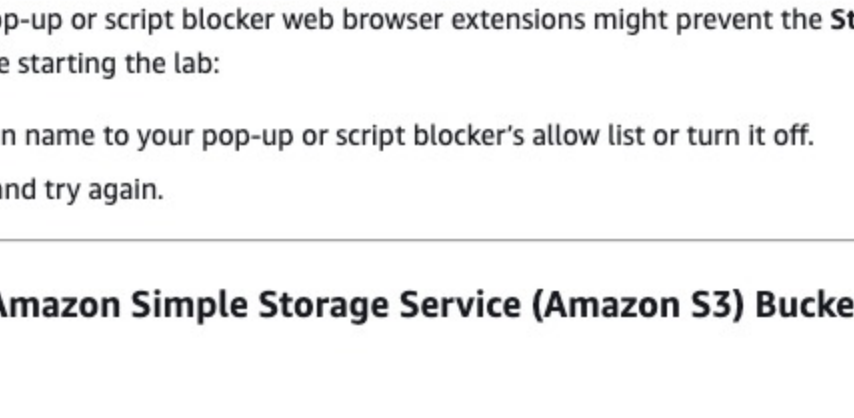
In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

- Add the lab domain name to your pop-up or script blocker's allow list or turn it off.
- Refresh the page and try again.

Task 1: Create an Amazon Simple Storage Service (Amazon S3) Bucket

INFRASTRUCTURE

To support the lab, we created some required resources for you. These resources include a VPC with two public subnets in two different Availability Zones, an Internet Gateway, a Route Table with a route to the Internet, and an EC2 instance hosting your employee directory application. See below for a resource overview:



Currently, the application runs in `Public Subnet 1`. The application does not have access to Amazon S3, but you provide that access later in this lab.

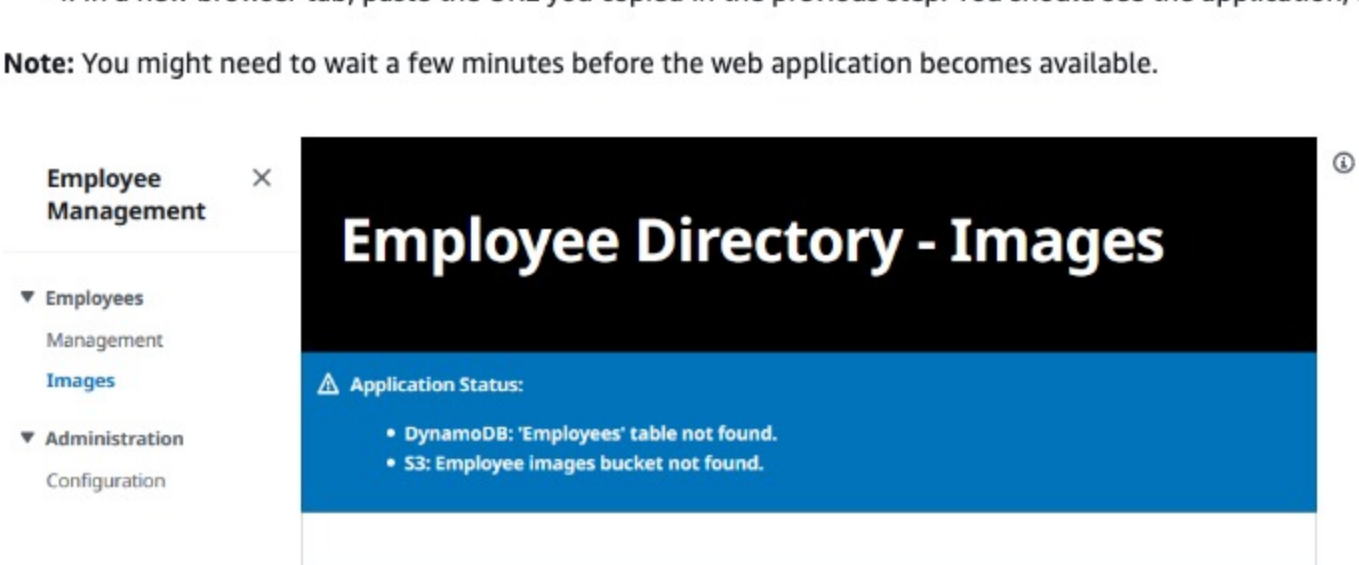
Applications must sign their API requests with AWS credentials to access other AWS resources. AWS Identity and Access Management (IAM) roles enable applications to make secure API requests to an instance, without requiring you to manage the security credentials that the applications use.

Instead of creating and distributing AWS credentials for the application, you can delegate permission to make API requests using IAM roles. In this lab, the application uses the `EmployeeDirectoryAppRole` IAM role. The role hasn't been configured to allow Amazon S3 access. The appication displays a warning message until Amazon S3 access is granted.

To access the employee directory application, do the following:

3. On the lab instructions page, in the left pane, copy `PublicWebApplicationURL`.
4. In a new browser tab, paste the URL you copied in the previous step. You should see the application, as shown.

Note: You might need to wait a few minutes before the web application becomes available.



A warning message states the following:

- *S3: Employee Images bucket not found.*
- *DynamoDB: 'Employees' table not found.*

First, you must address the S3 configuration. To fix this, you create an S3 bucket and upload images to it. You also configure a policy to allow the application IAM role to access the S3 bucket, allowing the application to display the images.

In this task, you create an S3 bucket. Every object in Amazon S3 is stored in an S3 bucket. When you create your bucket, make sure that you create the bucket in your specific lab Region. You can find the lab region on the instructions page, in the left pane.

5. At the top of the AWS Management Console, in the search bar, search for and choose `S3`.
6. Choose **Create bucket**, and then configure the following:

- **Bucket name:** `employee-photo-bucket-<INITIALS>-<NUMBER>`
  - Replace *INITIALS* with your initials
  - Replace *NUMBER* with a random, four-digit number
- For **Region**, make sure it matches the AWS Region value in the left pane of your instructions.

Example bucket name: `employee-photo-bucket-jwf-1234`

Note: Each S3 bucket name must be globally unique.

When you select a particular Region, you can optimize latency, minimize costs, and address regulatory requirements, as needed. Objects stored in a Region never leave that Region, unless you explicitly transfer them to another Region.

The **Copy settings from an existing bucket** option creates a bucket that uses the same settings as another bucket. For this lab, you do not use this option.

7. In the **Block Public Access settings for this bucket** section, examine the **Block all public access** section.

No changes are needed. The default setting is *checked*, ☑ **Block all public access**. This prevents all public access to data stored in the bucket.

8. Navigate to the bottom of the **Create bucket** page and choose **Create bucket**.

You should see a message similar to the following:

Successfully created bucket "employee-photo-bucket-XXX-XXXX"

Congratulations! You successfully created an Amazon S3 Bucket for your employee directory web application images.

In the next task, you create an Amazon S3 bucket policy.

Task 2: Create an S3 Bucket Policy

A *bucket policy* contains a set of permissions associated with an S3 bucket. The policy can control access to a entire bucket or to specific directories in a bucket.

9. Choose the `employee-photo-bucket-<INITIALS>-<NUMBER>` link for your bucket.
10. Choose the **Permissions** tab.
11. Navigate to the **Bucket policy** section, and then choose **Edit**.

The S3 Management Console presents a sample **Bucket policy editor**. Bucket policies can be created manually or they can be created with the assistance of the **AWS Policy Generator**. In this lab, you create the policy manually.

12. Copy and paste the following policy into the **Bucket policy editor**:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3ReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::INSERT-ACCOUNT-NUMBER:role/EmployeeDirectoryAppRole"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::INSERT-BUCKET-NAME",
        "arn:aws:s3:::INSERT-BUCKET-NAME/*"
      ]
    }
  ]
}
```

13. Replace the two `INSERT-BUCKET-NAME` placeholders with your bucket name, `employee-photo-bucket-<INITIALS>-<NUMBER>`.
14. In the left pane of the instructions, select and copy the value next to **AWSAccountID**.
15. Replace the `INSERT-ACCOUNT-NUMBER` placeholder with the **AWSAccountID** value copied in the previous step.

Your **bucket policy** should look similar to the following example:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3ReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::000000000000:role/EmployeeDirectoryAppRole"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::employee-photo-bucket-jwf-1234",
        "arn:aws:s3:::employee-photo-bucket-jwf-1234/*"
      ]
    }
  ]
}
```

16. Scroll to the bottom of the ""Edit bucket policy** page and choose **Save changes**.

Note: If you recieve an error regarding the first byte, ensure there is no empty space before the first `{` character on line 1. If there is, delete the empty space and try again.

If you policy is correct, you should receive a message similar to the following:

Successfully edited bucket policy

You applied a bucket policy to your S3 bucket. The bucket policy uses the `EmployeeDirectoryAppRole` IAM role to allow read access from your application to the S3 bucket. With this policy, all objects in your bucket are accessible to your application.

Congratulations! You successfully created a bucket policy for your Amazon S3 Bucket.

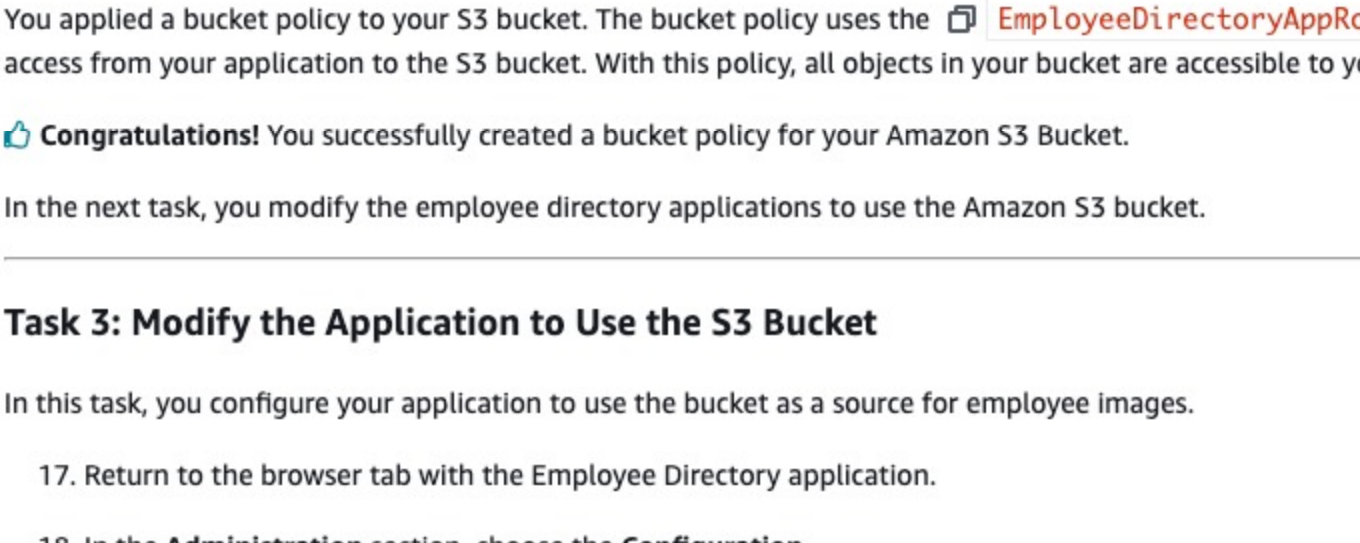
In the next task, you modify the employee directory applications to use the Amazon S3 bucket.

Task 3: Modify the Application to Use the S3 Bucket

In this task, you configure your application to use the bucket as a source for employee images.

17. Return to the browser tab with the Employee Directory application.
18. In the **Administration** section, choose the **Configuration**.

The **Configuration Settings** for the Employee Directory should look like this:

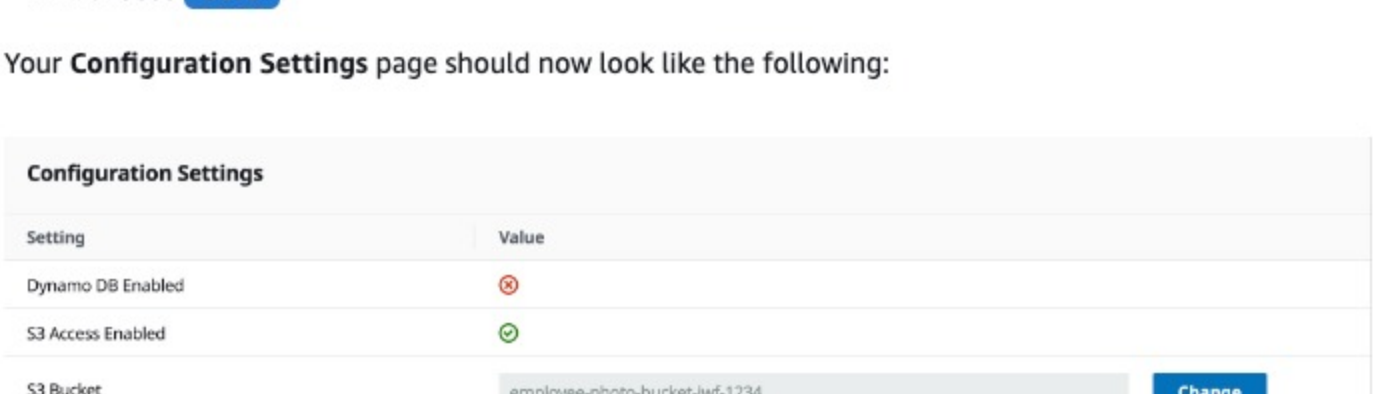


The **S3 Access Enabled** value ⊗ and blank **S3 Bucket** value indicate an S3 bucket has not been associated with the Employee Directory application.

Use the **Configuration Settings** section to associate your S3 bucket (`employee-photo-bucket-<INITIALS>-<NUMBER>`) with the application.

19. Choose **Change** in the **S3 Bucket** field.
20. Enter your bucket name (i.e. `employee-photo-bucket-<INITIALS>-<NUMBER>`) in the **S3 Bucket** field.
21. Choose **Save**.

Your **Configuration Settings** page should now look like the following:



The **S3 Access Enabled** value ⊘ and **S3 Bucket** value of `employee-photo-bucket-al-1234` indicate an S3 bucket has been successfully associated with the employee directory web application.

Congratulations! You successfully configured your employee directory web application to use an Amazon S3 Bucket to host your employee images.

In the next task, you upload the employee images to the Amazon S3 bucket.

Task 4: Upload an Object to an S3 Bucket

You created a bucket and granted permission to it from your EC2 Instance. Next, upload objects (images) to the Amazon S3 Bucket. An *object* can be any kind of file – text, photo, video, .zip, etc. When you add an object to an S3 bucket, you can include custom *metadata* with the object and set *permissions*, providinf granular access control.

In this task, you upload objects to your S3 bucket.

22. In the left pane in the lab instructions, copy the `PhotosZipURL` URL. Open it in a new browser tab and paste the URL in the new browser tab. This downloads a .zip file that contains 10 sample images.
23. Extract the compressed files to your computer, in a location of your choice.
24. Navigate to the extracted files to access the sample images. You should see 10 .png files in the directory.

Next, upload the images to your bucket.

25. Return to the browser tab displaying your S3 bucket and select the **Objects** tab.
26. Choose **Upload**.
27. In the **Files and Folders** section, choose **Add files**.
28. Browse to and select the .png files on your computer.
29. Choose **Open**.

You should see your selected files in the **Files and folders** section.

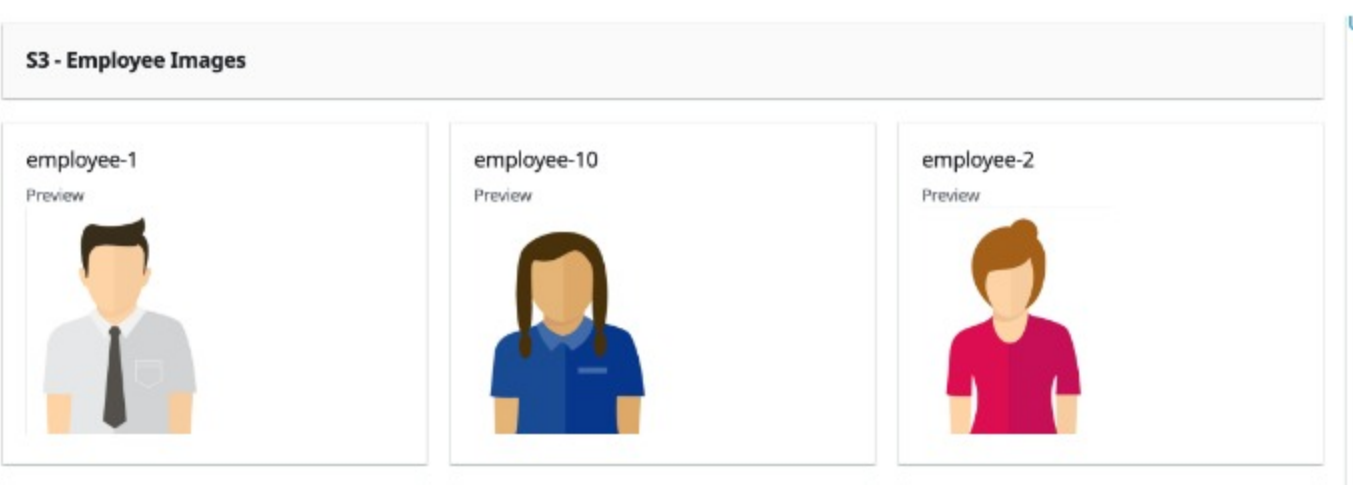
30. Navigate to the bottom of the **Upload** page and choose **Upload**.

You can see the upload progress. When the files are uploaded, you will see a message similar to the following:

Upload succeeded

31. Choose **Close** to return to the S3 dashboard.
32. Return to the browser tab with the Employee Directory application.
33. In the **Employees** section, choose **Images**.

The application displays the employee images you uploaded. It should look similar to the following image.



Congratulations! You successfully uploaded objects to your Amazon S3 Bucket and verified the employee direction application backend configuration.

In the next task, you create an Amazon DynamoDB table.

Task 5: Create an Amazon DynamoDB Table

Now that the S3 configuration is complete, the employee directory application is almost ready. But first, you must configure the application to present employee data using Amazon DynamoDB. In this task, you create a DynamoDB table to store all of your employee data for the employee directory application.

34. At the top of the AWS Management Console, in the search bar, search for and choose `DynamoDB`.
35. Choose **Create table**, and then configure the following:

Note: Depending on the size of the web browser screen, the **Create table** option may not be visible. If you do not see this option, select **Tables** in the right pane and select **Create table** before proceeding.

Important! Do not modify any other fields.

- **Table name:** `Employees`, use the the same capitalization shown.
- **Partition key:** `id`, select **String**.

36. Navigate to the bottom of the **Create table** page and choose **Create table**.

The table creation may take up to a minute. Wait until the table is successfully created before continuing. The status should show as follows:

Active

Congratulations! You successfully created a DynamoDB table.

In the next task, you test the employee directory application using the web application user interface.

Task 6: Test the Application Using the Application Web Interface

37. In your browser, go to the browser tab with the web application, and refresh the page.

Note: If you closed the browser tab, open a new one. From the left pane, copy `PublicWebApplicationURL`, and paste the URL into the address bar.

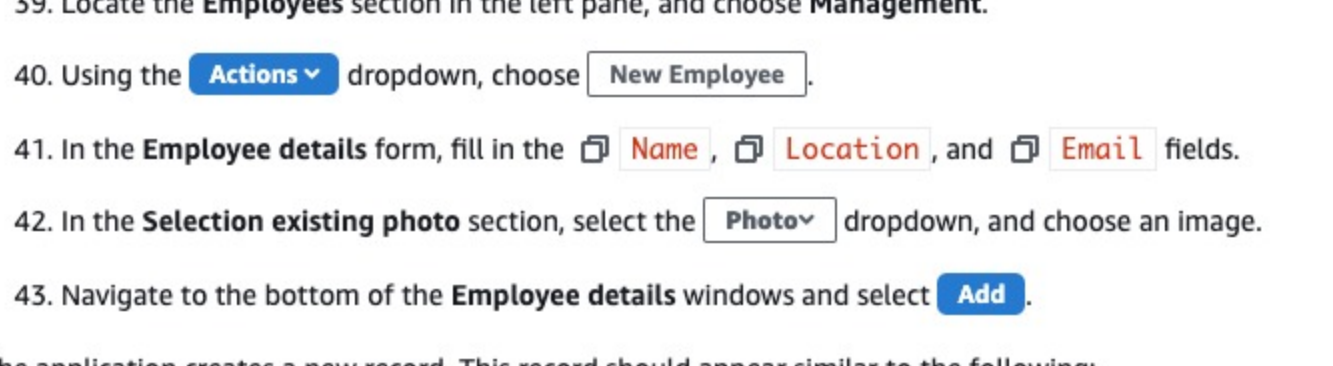
38. On the left side of the web application page, in the **Administration** section, choose **Configuration**.

Note: An IAM policy was created for you and attached to the EC2 instance that hosts the employee directory application. The role allows access to the DynamoDB table and allows you to see the DynamoDB table items from the application interface in your web browser.

Notice that the DynamoDB error is gone. This indicates that your employee directory application can now access your DynamoDB table.

39. Locate the **Employees** section in the left pane, and choose **Management**.
40. Using the **Actions** dropdown, choose **New Employee**.
41. In the **Employee details** form, fill in the `Name`, `Location`, and `Email` fields.
42. In the **Selection existing photo** section, select the **Photo** dropdown, and choose an image.
43. Navigate to the bottom of the **Employee details** windows and select **Add**.

The application creates a new record. This record should appear similar to the following:



44. For extra hands-on practice, create a few more employees, edit some items, and delete some items.

Congratulations! You successfully tested the employee directory application by adding, editing, and removing items from DynamoDB using the web interface.

In the next task, you manage existing DynamoDB items using the AWS Management Console.

Task 7: Manage Existing DynamoDB Items Using the AWS Management Console

In the next task, you validate that the your new employee data exists in your DynamoDB table and use the AWS Management Console to edit the data.

45. Return to the browser table with your DynamoDB table.
46. In the **Tables** section, choose the **Employees** link.
47. Review the **Employees** table details, including the Overview and Indexes tabs.
48. Choose **Explore table items**.

In the **Items returned** section, you can see the items in the database created from the application.

49. Choose an item to review by selecting the `id` column link.

The **Edit item** page returns the item attributes. Alternatively, to access the `JSON` representation, choose **JSON** at the top of the page.

You can use either view to edit the item attribute values.

Important: You will receive an error if you try to modify the primary key field, `id`. That field cannot be modified. To modify it, you must delete the item and add it again.

50. Update the *location* and *email* values in `JSON`, and then choose **Save changes**. You can also update the *photo* attribute but the name must be identical to the object in your S3 bucket.

Tip: As you make changes, go to your browser tab with the employee directory application and confirm that the changes return as they change in DynamoDB by refreshing the page.

Congratulations! You successfully managed existing items in your DynamoDB table and tested the changes in the employee directory application.

In the next task, you create items in a DynamoDB table using the AWS Management Console.

Task 8: Create Items in a DynamoDB Table Using the AWS Management Console

In this task, you use the AWS Management Console to create DynamoDB items in your table.

51. Go to your browser tab with the DynamoDB table.
52. In the **Items returned** section, choose **Create item**.

For the next steps, use the **Form** view.

53. In the **Attributes** section, provide a value for `id`. The `id` must be unique across all items in the table.
54. Choose **Add new attribute**, and select `String`.
55. Replace `NewValue` with `name`, and provide a value for **name**. For example, *John*.
56. Choose **Add new attribute**, and select `String`.
57. Replace `NewValue` with `location`, and provide a value for **location**. For example, *New York*.
58. Choose **Add new attribute**, and select `String`.
59. Replace `NewValue` with `email`, and provide a value for **email**. For example, *john.doe@example.org*.
60. Choose **Add new attribute**, and select `String`.
61. Replace `NewValue` with `photo`, and leave the field empty.
62. Choose **Create item**.

The DynamoDB console returns the following message:

The item has been saved successfully.

63. Go to your browser tab with the employee directory application and confirm that the new item displays in the **Employees** list by refreshing the page.
64. For more hands-on practice, create a few more employees, edit some items, and delete some items. Make sure that you provide the four required attributes: `name`, `location`, `email`, and (empty) `photo`.
65. Try to add a photo for each employee.

Congratulations! You successfully added new items to your DYnamoDB table using the AWS Management Console and testing the changes to the employee directory application.

Lab Complete

Congratulations! You can now:

- Create an Amazon Simple Storage Service (Amazon S3) Bucket
- Create an S3 bucket policy
- Modify an Application to Use an S3 Bucket
- Upload an Object to an S3 Bucket
- Create an Amazon DynamoDB table
- Test an Application Using an Application Web Interface
- Manage Existing DynamoDB Items Using the AWS Management Console
- Create Items in a DynamoDB Table Using the AWS Management Console

End lab

Follow these steps to close the console and end your lab.

66. Return to the **AWS Management Console**.
67. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
68. Choose **End lab** and then confirm that you want to end your lab.

Additional Resources

- For more information about Amazon S3, see Amazon S3.
- For more information about Amazon DynamoDB, see Amazon DynamoDB.
- For more information about editing object permissions, see Editing Object Permissions.