# Table of Contents

What Is AWS DeepLens? ................................................................. 1  
Device Versions ........................................................................... 1  
  The AWS DeepLens Device ....................................................... 1  
Hardware .................................................................................... 2  
Software ..................................................................................... 6  
How AWS DeepLens works .......................................................... 7  
Project workflow ....................................................................... 7  
Modeling Frameworks ................................................................. 7  
Getting Started .......................................................................... 9  
Register Your Device .................................................................. 9  
  Register AWS DeepLens 2019 Edition(v1.1) Device (v1.1) .......... 10  
  Register AWS DeepLens Device (v1) ...................................... 20  
Create and Deploy a Sample Project in the Console (~ 10 mins) ... 32  
Create and Deploy Your Project ................................................. 33  
Building Projects ....................................................................... 34  
Supported Frameworks ............................................................... 34  
  MXNet Models and Layers ...................................................... 34  
  TensorFlow Models and Layers ............................................. 36  
  Caffe Models and Layers ....................................................... 38  
Viewing Project Output .............................................................. 41  
  View Video Stream from AWS DeepLens Device in Browser .......... 42  
  View Video Streams on Your AWS DeepLens Device ............. 44  
  Creating a Lambda Function for Viewing the Project Stream ...... 46  
Working with Sample Projects .................................................... 49  
  Sample Projects Overview ...................................................... 49  
  Create and Deploy a Sample Project in the Console ................. 51  
  Relay Project Output through SMS ......................................... 53  
  Use SageMaker to Provision a Model for a Project .................. 59  
Working with Custom Projects .................................................... 69  
  Import Your SageMaker Trained Model .................................. 69  
  Import an Externally Trained Model ...................................... 69  
  Optimize a Custom Model ..................................................... 71  
  Create and Publish an Inference Lambda Function ................. 71  
  Create and Deploy a Custom Project ..................................... 75  
  Use Neo to Optimize Inference .............................................. 76  
Building Project Tutorials ........................................................... 78  
  Build and Run the Head Pose Detection Project .......... 79  
Managing Your Device ............................................................... 97  
  Securely Boot Your Device .................................................... 97  
  Update Your Device .............................................................. 97  
Deregistering Your AWS DeepLens Device ................................. 98  
Deleting AWS DeepLens Resources .......................................... 99  
  Delete Resources Using the Console .................................... 99  
Restoring AWS DeepLens to factory settings ............................... 100  
  Preparing to perform factory reset on your AWS DeepLens device .... 100  
  Restoring your AWS DeepLens device .................................. 106  
Logging and Troubleshooting ..................................................... 107  
  Project Logs ........................................................................ 107  
    CloudWatch Logs Log Groups ...................................... 107  
    File System Logs ........................................................... 108  
  Troubleshooting Guide ......................................................... 109  
  Troubleshooting Software on Device .................................. 109  

AWS DeepLens Developer Guide
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Registration of Device</td>
<td>114</td>
</tr>
<tr>
<td>Troubleshooting Model Deployments to Device</td>
<td>120</td>
</tr>
<tr>
<td>Device Library</td>
<td>124</td>
</tr>
<tr>
<td>awscam Module</td>
<td>124</td>
</tr>
<tr>
<td>getLastFrame Function</td>
<td>124</td>
</tr>
<tr>
<td>Model Object</td>
<td>125</td>
</tr>
<tr>
<td>mo Module</td>
<td>130</td>
</tr>
<tr>
<td>optimize Method</td>
<td>130</td>
</tr>
<tr>
<td>Troubleshooting the Model Optimizer</td>
<td>133</td>
</tr>
<tr>
<td>DeepLens_Kinesis_Video Module</td>
<td>139</td>
</tr>
<tr>
<td>createProducer Function</td>
<td>140</td>
</tr>
<tr>
<td>Producer Object</td>
<td>141</td>
</tr>
<tr>
<td>Stream Object</td>
<td>142</td>
</tr>
<tr>
<td>Security</td>
<td>144</td>
</tr>
<tr>
<td>Data Protection</td>
<td>144</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>144</td>
</tr>
<tr>
<td>Audience</td>
<td>145</td>
</tr>
<tr>
<td>Authenticating With Identities</td>
<td>145</td>
</tr>
<tr>
<td>Managing Access Using Policies</td>
<td>147</td>
</tr>
<tr>
<td>How AWS DeepLens Works with IAM</td>
<td>148</td>
</tr>
<tr>
<td>Identity-Based Policy Examples</td>
<td>150</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>156</td>
</tr>
<tr>
<td>Update Management</td>
<td>157</td>
</tr>
<tr>
<td>Security Compliance</td>
<td>157</td>
</tr>
<tr>
<td>AWS DeepLens End of Life</td>
<td>159</td>
</tr>
<tr>
<td>AWS DeepLens end of life FAQ</td>
<td>159</td>
</tr>
<tr>
<td>Delete your AWS DeepLens device resources</td>
<td>160</td>
</tr>
<tr>
<td>Delete your AWS DeepLens cloud resources</td>
<td>162</td>
</tr>
<tr>
<td>AWS DeepLens device troubleshooting</td>
<td>164</td>
</tr>
<tr>
<td>Document History</td>
<td>165</td>
</tr>
<tr>
<td>AWS glossary</td>
<td>167</td>
</tr>
</tbody>
</table>
What Is AWS DeepLens?

AWS DeepLens is a deep learning-enabled video camera. It is integrated with several AWS machine learning services and can perform local inference against deployed models provisioned from the AWS Cloud. It enables you to learn and explore the latest artificial intelligence (AI) tools and technology for developing computer vision applications based on a deep learning model.

As a beginner to machine learning, you can use AWS DeepLens to explore deep learning through hands-on tutorials based on deep learning sample projects. Each sample project contains a pre-trained model and a straightforward inference function.

As a seasoned practitioner, you can use the AWS DeepLens development environment to train a convolutional neural network (CNN) model and then deploy your computer vision application project containing the model to the AWS DeepLens device. You can train the model in any of the supported deep learning frameworks, including Caffe, MXNet, and TensorFlow.

To create and run an AWS DeepLens-based computer vision application project, you typically use the following AWS services:

- Use the SageMaker service to train and validate a CNN model or import a pre-trained model.
- Use the AWS Lambda service to create a project function to make inferences of video frames off the camera feeds against the model.
- Use the AWS DeepLens service to create a computer vision application project that consists of the model and inference function.
- Use the AWS IoT Greengrass service to deploy the application project and a Lambda runtime to your AWS DeepLens device, in addition to the software or configuration updates.

This means that you must grant appropriate permissions to access these AWS services.

Topics
- AWS DeepLens Device Versions (p. 1)
- AWS DeepLens Hardware (p. 2)
- AWS DeepLens Software (p. 6)

AWS DeepLens Device Versions

The following topics discuss the features and differences between the AWS DeepLens and AWS DeepLens 2019 Edition(v1.1) devices.

Topics
- The AWS DeepLens Device (p. 1)
- The AWS DeepLens 2019 Edition(v1.1) Device (p. 2)

The AWS DeepLens Device

First introduced at AWS re:Invent 2017, the AWS DeepLens device was made available in the US market on June 14, 2018.
For detailed hardware specifications, see [AWS DeepLens Hardware (p. 2)].

**The AWS DeepLens 2019 Edition(v1.1) Device**

The AWS DeepLens 2019 Edition(v1.1) device was made generally available on July 10, 2019 in the UK, Germany, France, Spain, Italy, Japan, Canada as well as US markets.

The AWS DeepLens 2019 Edition(v1.1) device includes the following hardware improvement:

- Simplified initial device setup through the USB-USB cable connection, instead of the SoftAP wireless connection.

For detailed hardware specification, see [AWS DeepLens Hardware (p. 2)].

**AWS DeepLens Hardware**

The AWS DeepLens device has the following specifications:

- A 4-megapixel camera with MJPEG (Motion JPEG)
- 8 GB of on-board memory
- 16 GB of storage capacity
- A 32-GB SD (Secure Digital) card
- Wi-Fi support for both 2.4 GHz and 5 GHz standard dual-band networking
- A micro HDMI display port
- Audio out and USB ports
- Power consumption: 20 W
- Power input: 5V and 4Amps

The following image shows the front and back of the AWS DeepLens hardware.
The following image shows the front and back of the AWS DeepLens 2019 Edition(v1.1) hardware.
On the front of the device, the power button is located at the bottom. Above it are three LED indicators show the device statuses:

- **Power status** indicates if the device is powered on or off.
- **Wi-Fi** shows if the device is in the setup mode (blinking), connected to your home or office network (steady) or not connected to the Internet (off).
- **Camera status**: when it is on, it indicates that a project is deployed successfully to the device and the project is running. Otherwise, the LED light is off.

On the back of the device, you have access to the following:

- A micro SD card slot for storing and transferring data.
- A micro HDMI slot for connecting a display monitor to the device using a micro-HDMI-to-HDMI cable.
- USB ports:
  - **AWS DeepLens**: Two USB 2.0 slots for connecting a USB mouse and keyboard, or any other USB-enabled accessories, to the device.
  - **AWS DeepLens 2019 Edition(v1.1)**: Two USB 3.0 slots, one for registration only and one for connecting a USB mouse and keyboard, or any other USB-enabled accessories, to the device.
**Note**

One of AWS DeepLens 2019 Edition(v1.1)'s USB slots is for registration only

- A reset pinhole for turning the device into the setup mode that allows you to make the device as an access point and to connect your laptop to the device to configure the device.
- An audio outlet for connecting to a speaker or earphones.
- A power supply connector for plugging in the device to an AC power source.

The AWS DeepLens camera is powered by an Intel® Atom processor, which can process 100 billion floating-point operations per second (GFLOPS). This gives you all of the computing power that you need to perform inference on your device. The micro HDMI display port, audio out, and USB ports allow you to attach peripherals, so you can get creative with your computer vision applications.

You can use AWS DeepLens as soon as you register it. Begin by deploying a sample project, and use it as a template for developing your own computer vision applications.

---

**AWS DeepLens Software**

The AWS DeepLens device uses the current versions of software for the following frameworks:

- Both hardware versions, 1.0 and 1.1, of the AWS DeepLens device support python 2.7 and Python 3.7.
- The supported deep learning AI architectures are MXNet 1.6.0 and TensorFlow 1.4.
How AWS DeepLens works

Learn about the basic workflow of a deployed AWS DeepLens project and AWS DeepLens's supported modeling frameworks.

AWS DeepLens Project workflow

The following diagram illustrates the basic workflow of a deployed AWS DeepLens project.

1. When turned on, the AWS DeepLens captures a video stream.
2. Your AWS DeepLens produces two output streams:
   - Device stream – The video stream passed through without processing.
   - Project stream – The results of the model's processing video frames
3. The Inference Lambda function receives unprocessed video frames.
4. The Inference Lambda function passes the unprocessed frames to the project's deep learning model, where they are processed.
5. The Inference Lambda function receives the processed frames from the model and passes the processed frames on in the project stream.

For more information, see Viewing AWS DeepLens Output Streams (p. 41).

Supported Modeling Frameworks

With AWS DeepLens, you train a project model using a supported deep learning modeling framework. You can train the model on the AWS Cloud or elsewhere. Currently, AWS DeepLens supports Caffe,
TensorFlow and Apache MXNet frameworks, in addition to Gluon models. For more information, see Machine Learning Frameworks Supported by AWS DeepLens (p. 34).
Getting Started with AWS DeepLens

In the following procedures, we walk you through securely connecting your AWS DeepLens and deploying your first models. Get started with an easy project that enables you to use your AWS DeepLens device to identify ordinary objects in 10 mins. When you're ready, try our more challenging cat identification tutorial, a template of the work flow for creating your own custom projects.

**Note**
To use the AWS DeepLens console and other AWS services, you need an AWS account. If you don't have an account, visit aws.amazon.com and choose Create an AWS Account. For detailed instructions, see Create and Activate an AWS Account.

After you've created your AWS account, sign in to the AWS DeepLens console, with your AWS account or user credentials. The topics in this section assume you've signed in to the AWS DeepComposer console.

**Topics**
- Register Your AWS DeepLens Device (p. 9)
- Create and Deploy a Sample Model (~ 10 mins) (p. 32)

Register Your AWS DeepLens Device

To run your deep learning computer vision application on your AWS DeepLens device, you must first register the device with AWS. After it's registered, you can create an AWS DeepLens project in the AWS Cloud. You'll also be able to deploy the project to the registered device and update the device software and settings.

The registration process is different for each version of the AWS DeepLens hardware. First, check the hardware version printed on the bottom of your AWS DeepLens device.

Then, choose one of the following links and follow the version-specific instructions.
Choose your device
- Register AWS DeepLens 2019 Edition(v1.1) Device (v1.1) (p. 10)
- Register Your AWS DeepLens Device (v1) (p. 20)

Register AWS DeepLens 2019 Edition(v1.1) Device (v1.1)

Registering your AWS DeepLens 2019 Edition(v1.1) device involves performing the following tasks:

1. Connect the device to your computer.
2. Verify the device serial number.
3. Set up the device's internet connection.
4. Create device representation in the AWS Cloud.
5. Update the device settings.

Follow the sections below for detailed instructions for each of the tasks.

Note
These instructions apply to the AWS DeepLens 2019 Edition(v1.1) device only. You can verify the hardware version on the bottom of your AWS DeepLens device. If you see HW v1.1, your device is the AWS DeepLens 2019 Edition(v1.1) v1.1. You can then proceed with the procedures in this section. Otherwise, see the section called “Register AWS DeepLens Device (v1)” (p. 20).

Topics
- Connect Your AWS DeepLens 2019 Edition(v1.1) Device to Your Computer (p. 10)
- Connect Your AWS DeepLens 2019 Edition(v1.1) Device to the Internet (p. 14)
- Name Your AWS DeepLens 2019 Edition(v1.1) Device and Complete the Registration (p. 16)
- View or Update Your AWS DeepLens 2019 Edition(v1.1) Device Settings (p. 19)

Connect Your AWS DeepLens 2019 Edition(v1.1) Device to Your Computer

To use a computer to register your AWS DeepLens 2019 Edition(v1.1) device, you must first connect the device to your computer. To connect your device to your computer, follow the steps in this section.

Note
In addition, you can also connect to the device directly using a monitor, a mouse and a keyboard (p. 13).

To connect your AWS DeepLens 2019 Edition(v1.1) device to your computer

2. Choose Register a device.
   
   Note
   If you don’t see a Register a device button, choose Devices from the main navigation pane.
3. In Choose a hardware version, choose HW v1.1 for your AWS DeepLens 2019 Edition(v1.1) device. Start to begin the registration.
4. On the **Connect your device to your computer** page, follow the instructions to power on your device and then connect the device to your computer by plugging one end of the USB-to-USB cable to a USB port into your computer and the other end into the device's **REGISTRATION** USB port on the back of the device. Then, choose **Next**.
5. Wait for the connection to complete when the **Device USB connection** status becomes **Connected** and then choose **Next**.
Connect to Your AWS DeepLens 2019 Edition (v1.1) Device Using a Monitor, Mouse, and Keyboard

As an alternative to using a computer to connect to your AWS DeepLens 2019 Edition (v1.1) device, you can also connect to the device directly using a monitor with a μHDMI-to-HDMI cable, a USB keyboard, and a USB mouse. You'll be prompted for the Ubuntu login credentials. If this is your first time you've logged in to the device using this method, enter `aws_cam` for Username and `aws_cam` for Password. When prompted, reset the password. For security reasons, use a strong password. For any subsequent logins, enter your new password in Password.

Validate Your AWS DeepLens 2019 Edition (v1.1) Device Serial Number

After your device is connected to your computer, the AWS DeepLens console validates the device serial number (DSN) to verify that the device is version 1.1.
To validate your AWS DeepLens 2019 Edition(v1.1) device

1. Make note of the last four digits of your device serial number. It's printed on the bottom of the device.
2. On the Validate your device page, enter the last four digits of your device serial number.
3. Choose Next.

Connect Your AWS DeepLens 2019 Edition(v1.1) Device to the Internet

After the device has been validated, you must get your AWS DeepLens 2019 Edition(v1.1) device connected to the internet. You can use a wireless (Wi-Fi) network or a wired (Ethernet) network. The latter requires that you have an Ethernet-to-USB adapter. The internet connection ensures that the device receive necessary software updates during registration.

Here, we demonstrate setting up the internet connection over Wi-Fi.

To set up the internet connection to your AWS DeepLens 2019 Edition(v1.1) device over Wi-Fi

1. On the Set up your device's internet connection page, choose Wi-Fi network under Network type.
2. Choose your network from the Wi-Fi network name (SSID), type your network password under Wi-Fi password, and then choose Connect.
3. Wait for the device to be connected to the internet, when **Status** under **Wi-Fi network details** becomes **Online**. Choose **Install software update** under **Required software update**.

4. Wait for the software update to complete, and then choose **Next**.
Name Your AWS DeepLens 2019 Edition(v1.1) Device and Complete the Registration

After your AWS DeepLens 2019 Edition(v1.1) device is connected to the internet and its software updated, name the device for future reference and agree to the AWS access permissions that are granted on your behalf in order to complete the registration.

To name your AWS DeepLens 2019 Edition(v1.1) device and complete the registration

1. Under Name your device, give the device a name.
2. Under Permissions, check the box to confirm I agree that required IAM roles containing necessary permissions be created on my behalf.
3. Choose Register device to complete the registration.
The device registration is now underway. The asynchronous process involves the following tasks:

- The device communicates with the AWS DeepLens service on the cloud through the specified Wi-Fi network.
- The AWS DeepLens service has necessary IAM roles with the required AWS permissions created for you.
- The AWS Cloud creates device representation with AWS IoT and other AWS services.
- The device downloads its AWS certificate of your account from the AWS Cloud.

**Verify Your AWS DeepLens 2019 Edition(v1.1) Device Registration**

After the registration is complete, verify the device registration is successful by checking the device's registration status.

**To verify your AWS DeepLens 2019 Edition(v1.1) device registration**

1. Wait for the device registration to complete. Make sure the **Registration status** under **Device Status** shows **Registered**.
2. Optionally, note the MQTT topic ID (e.g., $aws/things/deeplens_cTs8nnQxT0mX45HGLJ4DA/infer) displayed under **Project Output**. You’ll need this ID to view a deployed project output in the AWS IoT console.
View or Update Your AWS DeepLens 2019 Edition(v1.1) Device Settings

You can view or update the device settings once the device is successfully registered.

To view or update your AWS DeepLens 2019 Edition(v1.1) device settings

1. On the successfully registered device details page in the AWS DeepLens console, choose Edit device settings.
2. Make sure your device is connected to your computer via the USB-to-USB cable.
3. In Connect your device to your computer, choose Next.
4. After the Device USB connection status becomes Connected, choose Next again to open the Device settings page.

5. To use a different network for the device's internet connection, choose Edit in Network details. Choose a network type, choose a Wi-Fi network, type the password, and then choose Connect.
6. To enable SSH connection to the device and set the SSH password, choose Edit in SSH server. Choose Enable, create a password, confirm the password, and then choose Save changes.
7. To enable viewing video output from your device in a browser, install required video streaming certificates for one or more supported browsers.
   a. In Select your browser, choose a supported browser. For example, Firefox (Windows, MacOS Sierra or higher, and Linux).
   b. Choose Download streaming certificate to save the certificate to your computer.
   c. Follow the remaining steps to import the downloaded streaming certificate into the browser.

   **Note**
   Make sure you use DeepLens for the certificate password, when prompted.

To verify the certificate is installed properly, follow the instructions provided in View Video Streams from AWS DeepLens 2019 Edition(v1.1) Device in Browser (p. 41).
Register Your AWS DeepLens Device (v1)

The instructions presented thereafter apply to the original (also known as v1) AWS DeepLens device. You can find out the hardware version at the bottom of your AWS DeepLens device. If you don't see HW v1.1 printed there, your device is of the original AWS DeepLens edition. You can then proceed with the procedures in this section. Otherwise, see the section called “Register AWS DeepLens 2019 Edition(v1.1) Device (v1.1)” (p. 10).

The registration process involves performing the following tasks. Some of the tasks are carried out on the AWS Cloud and others are on the AWS DeepLens device.

- Name your device so that you can identify it within the AWS DeepLens service.
- Grant IAM permissions to build and deploy AWS DeepLens projects for deep learning computer vision applications.
- Download a security certificate for the device. This certificate is generated by AWS IoT upon request by the AWS DeepLens service. You must upload it to the device when setting up the device later.
- Create an AWS IoT thing representation for your AWS DeepLens device, which is carried out by AWS IoT Greengrass upon request by the AWS DeepLens service.
- Turn on the device's setup mode and join your computer in the device's local Wi-Fi (also referred to as AMDC-NNNN) network. This lets you call the device setup app as a web application hosted by the local web server of the device.
- Start the device setup application on the device to do the following:
  - Configure device access to internet.
  - Upload the AWS-generated security certificate to the device for the AWS Cloud to authenticate the device.
  - Create a device login password for signing in to the device using a hardwired monitor, mouse, and keyboard, or using an SSH client from a computer within the same home or office network.

Your AWS DeepLens device has a default password of aws_cam. You can use this default device password to log on to the device connected to a monitor using a μUSB-to-USB cable, a USB mouse and possibly a USB keyboard even before registration. For security reasons, you should reset this password with a more complex or strong password phrase.

Topics

- Configure Your AWS Account for AWS DeepLens Device (p. 20)
- Connect to Your AWS DeepLens Device's Wi-Fi Network (p. 23)
- Set Up Your AWS DeepLens Device (p. 27)
- Verify Your AWS DeepLens Device Registration Status (p. 31)

Configure Your AWS Account for AWS DeepLens Device

Configuring your AWS account for your AWS DeepLens device involves naming the device, grant AWS access permissions, and download a certificate for the device to be authenticated by AWS.

To configure your AWS account for AWS DeepLens device

2. Choose **Register a device**. If you don't see a **Register a device** button, choose **Devices** on the main navigation pane.

3. On the **Choose a hardware version** dialog window, choose the **HW v1** radio button for your AWS DeepLens device. Then choose **Start**.

4. In the **Name your device** section on the **Configure your AWS account** page, type a name (e.g., My-DeepLens-1) for your AWS DeepLens device in the **Device name** text field.

   The device name can have up to 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen) only.

![Configure your AWS account](image)

5. In the **Certificate** section, choose **Download certificate** to save the device certificate.

   **Important**
   The downloaded device certificate is a .zip file. Don't unzip it.
Certificates aren't reusable. You must generate a new certificate every time you register your device.

6. After the certificate is downloaded, choose Next to proceed to joining your computer to your device's (AMDC-NNNN) Wi-Fi network in order to start the device setup application hosted on the device.

**Note**

On devices of certain earlier versions, the legacy device setup app assumes that your home or office Wi-Fi network's name (SSID) and password do not contain special characters, including space, backward slash (\), single quote ('), double quote ("), or colon (:). If you've got such a device and your home or office Wi-Fi network name or password contains such special characters, the legacy device setup app will be blocked when you attempt to configure its network connection.

If you have such a legacy device, after choosing Next, you will be prompted with a modal dialog to review requirements for your home or office Wi-Fi network, as shown as follows:

![Modal dialog](image)

- If your home or office network name or password contains any special character, choose Yes, my network has special characters and follow this troubleshooting guide (p. 116) to establish an SSH session to configure the Wi-Fi network connection between your device and the internet and, then, to move on to configuring the rest of the device settings. After that, you should update the device software to its latest version.

- If your home or office network name or password do not contain any special character, choose No, my network has no special characters to be directed to the Connect to your device page (p. 23).

If you have a more recent device or your device software is updated, you will be directed to the Connect to your device page (p. 23) without the modal dialog after choosing Next.
Register AWS DeepLens Device (v1)

Connect to Your AWS DeepLens Device's Wi-Fi Network

To set up your AWS DeepLens device, you must first connect your computer to the device's local Wi-Fi network, also known as the device's AMDC-NNNN network. When the Wi-Fi indicator (the middle LED light) blinks on the front of the device, this network is active and the device is in setup mode. You're then ready to connect a computer to the device.

**Note**
In addition, you can also connect to the device directly using an external monitor, mouse and keyboard (p. 27).

When you set up your device for the first time, the device is automatically booted into setup mode and ready for your computer to join its AMDC-NNNN network. To update device settings after the initial setup, you must explicitly turn on the device setup mode (instructions given below) and then have your computer rejoin the device's Wi-Fi network. If the device exits setup mode before you can finish the setup, you must reconnect your computer to the device in the same way.

While your AWS DeepLens device is in its setup mode and your computer is a member of its Wi-Fi network, you can open the device setup application, an HTML page hosted on the device's local web server, to configure the device settings. The device remains in setup mode for up to 2 hours, giving you enough time to finish configuring the device. When the setup is complete or has exceeded 2 hours, the device will exit setup mode and the Wi-Fi indicator stops blinking. The AMDC-NNNN network is then deactivated and your computer disconnected from that network and reconnected to its home or office network.

**To connect to your AWS DeepLens device's Wi-Fi network**

1. Look at the bottom of your device and make note of the device's AMDC-NNNN network SSID and password.

   ![Device Bottom with Network Information]

2. Plug in your AWS DeepLens device to an AC power outlet. Press the power button on the front of the device to turn the device on.
3. Wait until the device has entered into setup mode when the Wi-Fi indicator (middle LED) on the front of the device starts to flash.

**Note**
If Wi-Fi indicator does not flash, the device is no longer in the setup mode. To turn on the device's setup mode again, press a paper clip into the reset pinhole on the back of the device. After you hear a click, wait about 20 seconds for the Wi-Fi indicator to blink.

4. Open the network management tool on your computer. Choose your device's SSID from the list of available Wi-Fi networks and type the password for the device's network. The SSID and password are printed on the bottom of your device. The device's Wi-Fi network's SSID has the AMDC-NNNN format.

On a computer running Windows, choose **Connecting using a security key instead** instead of **Enter the PIN from the router label (usually 8 digits)** and then enter your device's Wi-Fi password.
After successfully connecting your computer to the device's Wi-Fi network, you're now ready to launch the device setup application to configure your device (p. 27).

To launch the device setup app, do one of the following:

- For the initial registration using the AWS DeepLens console, go back to the Connect to your device page and choose Next.
Connect to your device

Now that you have configured your AWS account, you will connect to network access and upload the security certificate to finish registration.

Connect your computer to your device's Wi-Fi

1. Plug in and power on
Plug in and press the power button to turn on your AWS DeepLens. The power indicator, the bottom LED, will turn on.

2. Verify middle LED is blinking
When the middle LED is blinking, AWS DeepLens is in setup mode. Note- this may take about 20 seconds after power on.

Middle LED is not blinking?
Make sure your AWS DeepLens is plugged in and powered on.

If the middle LED is still not blinking, you can manually insert a paperclip into the small hole marked 'reset' on the back for about 20 seconds and the wireless network status.
For updating the device settings after the initial registration, open a web browser tab and enter http://deeplens.amazon.net or http://deeplens.config in the address bar.

**Note**
If the above URL doesn't work, your AWS DeepLens device may have the awscam software version 1.3.5 or earlier installed. In this case, update the device software and try it again. Alternatively, instead of http://deeplens.amazon.net or http://deeplens.config, you can open the device setup page by using one of the following URLs, depending on the software version on your AWS DeepLens device.

- http://192.168.0.1, if the AWS DeepLens software package (awscam) version is less than 1.2.4
- http://10.105.168.217, if the AWS DeepLens software package (awscam) version is greater than or equal to 1.2.4

For more information, see Device Setup URL (p. 119).

Connect to AWS DeepLens Device Using Monitor, Mouse and Keyboard

In addition to using a computer to connect to your AWS DeepLens device, you can also connect to the device directly using a monitor with a μHDMI-to-HDMI cable, a USB keyboard and/or a USB mouse. You'll be prompted for the Ubuntu login credentials. Enter awscam in **username**. When logging to the device for the first time, use the default password of awscam in **password**. You'll then be asked to reset the password. For security reasons, use a strong password of a complex phrase. For any subsequent logins, use the reset password.

Set Up Your AWS DeepLens Device

When setting up your AWS DeepLens device, you perform the following tasks while your computer is connected to your device's AMDC-NNNN network:

- Enable the device's internet connection through your home or office wireless (Wi-Fi) or wired (Ethernet) network.
- Attach to your device the AWS-provisioned security certificate as discussed in the section called “Register Your Device” (p. 9).
- Set up login access to the device, including with an SSH connection or a wired connection.
- Optionally, download the streaming certificate from the device to enable viewing project video output in a supported browser.

If your computer is no longer a member of the AMDC-NNNN network because your AWS DeepLens device has exited setup mode, follow the instructions in the section called “Connect to Device” (p. 23) to establish a connection and to open the device setup page, again, before proceeding further.

To set up your AWS DeepLens device

1. If your AWS DeepLens device has a more recent version of the software installed, you won't be prompted with the following tasks. Skip to Step 2 below. Otherwise, proceed to the Device setup page, which you opened after connecting to the device (p. 23), to set up your home or office network to connect your device to the internet:

   a. Under **Step 1: Connect to network**, choose your home or office Wi-Fi network SSID from the **Wi-Fi network ID** drop-down list. Type the Wi-Fi network password
Alternatively, You can choose **Use Ethernet** to connect your AWS DeepLens device to the internet.

b. Choose **Next** to connect the device to the internet.

c. On the next page, Choose **Install and reboot** to install the latest software on the device and to restart the device.
After the software update is installed and the device restarted, reconnect your computer to your device’s AMDC-NNNN network, navigate to http://deeplens.config in a web browser to open the updated device setup application, and to complete the rest of the device setup as shown in Step 2.

2. When your device has an updated software installed, starting the device setup application (e.g., http://deeplens.config) opens a browser page similar to the following:
Configure your AWS DeepLens

You are now connected to your AWS DeepLens. In this step, you will connect the device to your home or office network, set a password to access your device.

Connect your device to your home or office network

In order to complete device registration, you need to connect your device to the internet. You can use Wi-Fi or wired (Ethernet-USB adapter). If connecting to your office network, make sure AWS DeepLens can access the Internet through ports 8883 and 8884.

- Wireless network SSID
  - Haymuto
    - Status: Online

- Wired connection
  - Ethernet-USB Adapter
    - Status: Online

Upload security certificate to associate your AWS DeepLens to your AWS account

To enable your device to connect to AWS, browse to the security certificate that you downloaded previously. By default, the certificate is in your Downloads directory. Upload the .zip file.

- Attached certificate
  - certificates-deeplens_h0_PU0ccTzG4k2G26Aaw50.zip

Set a password to control how you access and update the device

You are required to setup a password to protect login access to your device. If you forget your password, you will lose access to your device and can re-enable access by performing a factory reset, but you will lose any data store on your device.

- Device password: ***************

SSH server

- Enabled

By clicking Finish below, you agree to the terms (https://aws.amazon.com/deeplens/terms/) covering your use of AWS DeepLens.
The Connect your device to your home or office network section shows the device's internet connection status as Online. You can choose Edit to update the internet connection by choosing a different Wi-Fi network or a wired network with a micro-USB-to-Ethernet adaptor. Otherwise, continue to the next step to complete the rest of the device configuration.

3. Under Upload security certificate to associate your AWS DeepLens to your AWS account on the updated Configure your AWS DeepLens page, do the following:
   a. Choose Browse to open a file picker.
   b. Locate and choose the security certificate that you downloaded when preparing your AWS account for AWS DeepLens (p. 9).
   c. Choose Upload zip file to attach the certificate to the device.

   **Note**
   The downloaded security certificate for the device is a .zip file. Upload the unzipped certificate file as-is.

For device setup update after the initial registration, your device has a previous certificate installed. In this case, choose Edit and follow the instructions above in this step to upload the new certificate.

4. Under Set a password to control how you access and update the device, complete the following steps to configure device access.
   a. For the initial registration, type a password in Create a password. The password must be at minimum eight characters long and contain at least one number, an uppercase letter, and a special character (e.g., ‘$’, ‘&’, ‘#’, ‘$', ‘%’, ‘@’, or ‘!’). You need this password to log in to your device either using an SSH connection (if enabled below) or using a hardwired monitor, a USB mouse and/or a USB keyboard.
   b. For SSH server, choose Enable or Disable. If enabled, SSH allows you to log in to your device using an SSH terminal on your Mac or Linux computer or using PuTTY or another SSH client on your Windows computer.

   For subsequent configuration updates after the initial registration, you can choose Edit and follow the ensuing instructions to update the password.

5. Optionally, on the upper-right corner of the device setup page, choose Enable video streaming to enable viewing project video output using a supported browser. For the initial registration, we recommend that you skip this option and enable it later when updating the device configuration after you've become more familiar with AWS DeepLens.

6. Review the settings. Then, choose Finish to complete setting up the device and to terminate your connection to the device's Wi-Fi network. Make sure to connect your computer back to your home or office network.

   **Note**
   To ensure the setup completes successfully, make sure that AWS DeepLens device has access to ports 8883 and 8443 and is not blocked by your network firewall policy.
   If the AWS DeepLens device's connection to the internet repeatedly turns on and off after you chose Finish, restart your home or office Wi-Fi network.

This completes the device registration. Verify your device registration status (p. 31) before moving on to create and deploy a project to your AWS DeepLens device.

**Verify Your AWS DeepLens Device Registration Status**

After the device setup is complete, choose Open AWS DeepLens console to verify the registration status.
Device registration takes a few minutes to process. When the registration completes successfully, **Registration status** changes to **Registered**. If the process fails, **Registration status** becomes **Failed**. In this case, choose **Deregister** and then start the registration all over again. When the registration is interrupted or otherwise incomplete, **Registration status** remains **Awaiting credentials**. In this case, reconnect to the device's AMDC-NNNN Wi-Fi network (p. 23) to resume the registration.

When the device's **Registration status** and **Device status** becomes **Registered** and **Online**, respectively, you're ready to create and deploy a project to your AWS DeepLens device.

**Create and Deploy a Sample Model (~ 10 mins)**

In this walkthrough, you'll use the AWS DeepLens console to create an AWS DeepLens project from the Object Detection sample project template (p. 49) to create an AWS DeepLens project. The pre-trained object detection model can analyze images from a video stream captured on your AWS DeepLens device and identify an objects as one of as many as 20 labeled image types. The instructions presented here apply to creating and deploying other AWS DeepLens sample projects.

The following diagram presents a high-level overview of the processes to use the AWS DeepLens console to create and deploy a sample project.
When creating a sample project, the fields in the console are pre-populated for you so you can accept the defaults. In the **Project content** portion of the screen, you need to know the project's model and inference function. You can find the information for the individual projects in [AWS DeepLens Sample Projects Overview](#).  

**Create and Deploy Your Project**

Follow the steps in this procedure to create and deploy the Object Detection sample project.

**To create and deploy an AWS DeepLens sample project using the AWS DeepLens console**

2. Choose **Projects**, then choose **Create new project**.
3. On the **Choose project type** page, do the following:
   a. Choose **Use a project template**, then choose the sample project you want to create. For this exercise, choose **Object detection**.
   b. Scroll to the bottom of the screen, then choose **Next**.
4. On the **Specify project details** page, do the following:
   a. In the **Project information** section, do the following:
      i. Either accept the default name for the project, or enter a name you prefer.
      ii. Either accept the default description for the project, or enter a description you prefer.
   b. Choose **Create**.
      This returns you to the **Projects** page where the project you just created is listed with your other projects.
5. On the **Projects** page, choose the radio button to the left of your project name or choose the project to open the project details page, then choose **Deploy to device**.
6. On the **Target device** page, from the list of AWS DeepLens devices, choose the device that you want to deploy this project to. An AWS DeepLens device can have only one project deployed to it at a time.
7. Choose **Review**.
   If a project is already deployed to the device, you will see an error message that deploying this project will overwrite the project that is already running on the device. Choose **Continue project**.
8. On the **Review and deploy** screen, review your project and choose either **Previous** to go back and make changes, or **Deploy** to deploy the project.
   **Important**  
   Deploying a project incurs costs for the AWS services that are used to run the project.

For instructions on viewing your project's output, see [Viewing AWS DeepLens Output Streams](#).
Building AWS DeepLens Projects

When your AWS DeepLens device is registered with and connected to the AWS Cloud, you can begin to create an AWS DeepLens project on the AWS Cloud and deploy it to run on the device. An AWS DeepLens project is a deep learning-based computer vision application. It consists of a deep learning model and a Lambda function to perform inference based on the model.

Before creating an AWS DeepLens project, you must have trained or have someone else trained a deep learning model using one of the supported machine learning frameworks (p. 34). The model can be trained using SageMaker or another machine learning environment. In addition, you must also have created and published an inference function in AWS Lambda. In this chapter, you'll learn how to train a computer vision deep learning model in SageMaker and how to create an inference Lambda function to make inferences and to implement other application logic.

To help you learn building your AWS DeepLens project, you have access to a set of AWS DeepLens sample projects. You can use the sample projects as-is to learn programming patterns for building a AWS DeepLens project. You can also use them as templates to extend their functionality. In this chapter, you'll learn more about these sample projects and how to employ one to run on your device, as well.

Topics
- Machine Learning Frameworks Supported by AWS DeepLens (p. 34)
- Viewing AWS DeepLens Output Streams (p. 41)
- Working with AWS DeepLens Sample Projects (p. 49)
- Working with AWS DeepLens Custom Projects (p. 69)
- Building AWS DeepLens Project Tutorials (p. 78)

Machine Learning Frameworks Supported by AWS DeepLens

AWS DeepLens supports deep learning models trained using the Apache MXNet (including support for Gluon API), TensorFlow, and Caffe frameworks. This section lists the models and modeling layers that AWS DeepLens supports for each framework.

Topics
- Supported Apache MXNet Models and Supporting MXNet Layers (p. 34)
- Supported TensorFlow Models and Supporting TensorFlow Layers (p. 36)
- Supported Caffe Models and Supporting Caffe Layers (p. 38)

Supported Apache MXNet Models and Supporting MXNet Layers

AWS DeepLens supports Apache MXNet deep learning models that are exposed by the Gluon API and MXNet layers. This section lists the supported models and layers.

Topics
- Supported MXNet Models Exposed by the Gluon API (p. 35)
- Supporting MXNet Layers (p. 35)
Supported MXNet Models Exposed by the Gluon API

AWS DeepLens supports the following Apache MXNet deep learning models from the Gluon model zoo that are exposed by the Gluon API.

<table>
<thead>
<tr>
<th>Supported Gluon Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlexNet</td>
<td>Image classification model trained on the ImageNet dataset imported from the Open Neural Network Exchange (ONNX).</td>
</tr>
<tr>
<td>ResNet</td>
<td>Image classification model trained on the ImageNet dataset imported from MXNet.</td>
</tr>
<tr>
<td>SqueezeNet</td>
<td>Image classification model trained on the ImageNet dataset imported from ONNX.</td>
</tr>
<tr>
<td>VGG</td>
<td>Image classification model trained on the ImageNet dataset imported from MXNet or ONNX.</td>
</tr>
</tbody>
</table>

Example

The following example shows how to export a SqueezeNet version 1 model using the Gluon API. The output is a symbol and parameters file. The filename has the 'squeezenet' prefix.

```python
import mxnet as mx
from mxnet.gluon.model_zoo import vision
squeezenet = vision.squeezenet_v1(pretrained=True, ctx=mx.cpu())

# To export, you need to hybridize your gluon model,
squeezenet.hybridize()

# SqueezeNet’s input pattern is 224 pixel X 224 pixel images. Prepare a fake image,
fake_image = mx.nd.random.uniform(shape=(1,3,224,224), ctx=mx.cpu())

# Run the model once.
result = squeezenet(fake_image)

# Now you can export the model. You can use a path if you want ‘models/squeezenet’.
squeezenet.export('squeezenet')
```

For a complete list of models and more information, see the [Gluon Model Zoo](https://gluon-cnn.mxnet.io/).

Supporting MXNet Layers

You can use the following Apache MXNet modeling layers to train deep learning model for AWS DeepLens.

<table>
<thead>
<tr>
<th>Supported MXNet Modeling Layers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation</td>
<td>Applies an activation function to the input</td>
</tr>
</tbody>
</table>
### Supported MXNet Modeling Layers

<table>
<thead>
<tr>
<th>Layer Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BatchNorm</td>
<td>Applies batch normalization</td>
</tr>
<tr>
<td>Concat</td>
<td>Joins input arrays along a given axis</td>
</tr>
<tr>
<td>_contrib_MultiBoxDetection</td>
<td>Converts a multibox detection prediction</td>
</tr>
<tr>
<td>_contrib_MultiBoxPrior</td>
<td>Generates prior boxes from data, sizes, and ratios</td>
</tr>
<tr>
<td>Convolution</td>
<td>Applies a convolution layer on input</td>
</tr>
<tr>
<td>Deconvolution</td>
<td>Applies a transposed convolution on input</td>
</tr>
<tr>
<td>elemwise_add</td>
<td>Applies element-wise addition of arguments</td>
</tr>
<tr>
<td>Flatten</td>
<td>Collapses the higher dimensions of an input into an 2-dimensional array</td>
</tr>
<tr>
<td>FullyConnected</td>
<td>Applies a linear transformation of $Y = WX + b$ on input $X$</td>
</tr>
<tr>
<td>InputLayer</td>
<td>Specifies the input to a neural network</td>
</tr>
<tr>
<td>L2Norm</td>
<td>Applies L2 normalization to the input array</td>
</tr>
<tr>
<td>LRN (Local Response Normalization)</td>
<td>Applies local response normalization to the input array</td>
</tr>
<tr>
<td>Pooling</td>
<td>Performs pooling on the input</td>
</tr>
<tr>
<td>Reshape</td>
<td>Reshapes the input array with a different view without changing the data</td>
</tr>
<tr>
<td>ScaleShift</td>
<td>Applies scale and shift operations on input elements</td>
</tr>
<tr>
<td>SoftmaxActivation</td>
<td>Applies Softmax activation to the input</td>
</tr>
<tr>
<td>SoftmaxOutput</td>
<td>Computes the gradient of cross-entropy loss with respect to Softmax output</td>
</tr>
<tr>
<td>transpose</td>
<td>Permutes the dimensions of an array</td>
</tr>
<tr>
<td>UpSampling</td>
<td>Performs nearest-neighbor or bilinear upsampling to input</td>
</tr>
<tr>
<td>_mul</td>
<td>Performs multiplication</td>
</tr>
<tr>
<td>_Plus</td>
<td>Performs an element-wise sum of the input arrays with broadcasting</td>
</tr>
</tbody>
</table>

For more information about MXNet layers, see [MXNet Gluon Neural Network Layers](#).

### Supported TensorFlow Models and Supporting TensorFlow Layers

AWS DeepLens supports the following TensorFlow models and layers for deep learning.

**Topics**
- [Supported TensorFlow Models (p. 37)](#)
• Supporting TensorFlow Layers (p. 37)

Supported TensorFlow Models

AWS DeepLens supports the following deep learning models that have been trained with TensorFlow.

<table>
<thead>
<tr>
<th>Supported TensorFlow Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inception</strong></td>
</tr>
<tr>
<td>An image classification model trained on the ImageNet dataset using TensorFlow</td>
</tr>
<tr>
<td><strong>MobileNet</strong></td>
</tr>
<tr>
<td>An image classification model trained on the ImageNet dataset using TensorFlow</td>
</tr>
<tr>
<td><strong>NasNet</strong></td>
</tr>
<tr>
<td>An image classification model trained on the ImageNet dataset using TensorFlow</td>
</tr>
<tr>
<td><strong>ResNet</strong></td>
</tr>
<tr>
<td>An image classification model trained on the ImageNet dataset using TensorFlow</td>
</tr>
<tr>
<td><strong>VGG</strong></td>
</tr>
<tr>
<td>An image classification model trained on the ImageNet dataset using TensorFlow</td>
</tr>
</tbody>
</table>

For more information about TensorFlow models, see tensorflow/models on GitHub.

Supporting TensorFlow Layers

You can use the following TensorFlow layers to train deep learning models that are supported by AWS DeepLens.

<table>
<thead>
<tr>
<th>Supported TensorFlow Layers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
</tr>
<tr>
<td>Computes element-wise addition</td>
</tr>
<tr>
<td><strong>AvgPool</strong></td>
</tr>
<tr>
<td>Performs average pooling on the input</td>
</tr>
<tr>
<td><strong>BatchToSpaceND</strong></td>
</tr>
<tr>
<td>Rearranges data from batch into blocks of spatial data</td>
</tr>
<tr>
<td><strong>BiasAdd</strong></td>
</tr>
<tr>
<td>Adds bias</td>
</tr>
<tr>
<td><strong>Const</strong></td>
</tr>
<tr>
<td>Creates a constant tensor</td>
</tr>
<tr>
<td><strong>Conv2D</strong></td>
</tr>
<tr>
<td>Computes a 2-D convolution</td>
</tr>
<tr>
<td><strong>Conv2DBackpropInput</strong></td>
</tr>
<tr>
<td>Computes the gradients of convolution with respect to the input</td>
</tr>
<tr>
<td><strong>Identity</strong></td>
</tr>
<tr>
<td>Returns a tensor with the same shape and contents as input</td>
</tr>
<tr>
<td><strong>Maximum</strong></td>
</tr>
<tr>
<td>Computes element-wise maximization.</td>
</tr>
<tr>
<td><strong>MaxPool</strong></td>
</tr>
<tr>
<td>Performs the max pooling on the input</td>
</tr>
<tr>
<td><strong>Mean</strong></td>
</tr>
<tr>
<td>Computes the mean of elements across dimensions of a tensor</td>
</tr>
<tr>
<td><strong>Mul</strong></td>
</tr>
<tr>
<td>Computes element-wise multiplication</td>
</tr>
<tr>
<td><strong>Neg</strong></td>
</tr>
<tr>
<td>Computes numerical negative value element-wise</td>
</tr>
</tbody>
</table>
## Supported TensorFlow Layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pad</td>
<td>Pads a tensor</td>
</tr>
<tr>
<td>Placeholder</td>
<td>Inserts a placeholder for a tensor that will be always fed</td>
</tr>
<tr>
<td>Prod</td>
<td>Computes the product of elements across dimensions of a tensor</td>
</tr>
<tr>
<td>RandomUniform</td>
<td>Outputs random values from a uniform distribution</td>
</tr>
<tr>
<td>Range</td>
<td>Creates a sequence of numbers</td>
</tr>
<tr>
<td>Relu</td>
<td>Computes rectified linear activations</td>
</tr>
<tr>
<td>Reshape</td>
<td>Reshapes a tensor</td>
</tr>
<tr>
<td>Rsqrt</td>
<td>Computes reciprocal of square root</td>
</tr>
<tr>
<td>Shape</td>
<td>Returns the shape of a tensor</td>
</tr>
<tr>
<td>Softmax</td>
<td>Computes Softmax activations</td>
</tr>
<tr>
<td>SpaceToBatchND</td>
<td>Zero-pads and then rearranges blocks of spatial data into batch</td>
</tr>
<tr>
<td>Square</td>
<td>Computes element-wise square</td>
</tr>
<tr>
<td>Squeeze</td>
<td>Removes dimensions of size 1 from the shape of a tensor</td>
</tr>
<tr>
<td>StopGradient</td>
<td>Stops gradient computation</td>
</tr>
<tr>
<td>Sub</td>
<td>Computes element-wise subtraction</td>
</tr>
<tr>
<td>Sum</td>
<td>Computes the sum of elements across dimensions of a tensor</td>
</tr>
<tr>
<td>Tile</td>
<td>Constructs a tensor by tiling a given tensor</td>
</tr>
</tbody>
</table>

For more information about TensorFlow layers, see [TensorFlow Layers](#).

### Supported Caffe Models and Supporting Caffe Layers

AWS DeepLens supports the following deep learning models trained with Caffe and Caffe modeling layers.

#### Topics
- [Supported Caffe Models (p. 38)](#)
- [Supporting Caffe Layers (p. 39)](#)

### Supported Caffe Models

AWS DeepLens supports the following deep learning models trained with Caffe.

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlexNet</td>
<td>An image classification model trained on the ImageNet dataset using Caffe</td>
</tr>
<tr>
<td>DenseNet</td>
<td>An image classification model from the original Torch model</td>
</tr>
</tbody>
</table>
Supported Caffe Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inception</td>
<td>An image classification model converted from the original Apache MXNet model</td>
</tr>
<tr>
<td>MobileNet</td>
<td>An image classification model trained on the ImageNet dataset using Caffe</td>
</tr>
<tr>
<td>ResNet</td>
<td>An image classification model trained on the ImageNet dataset using Caffe</td>
</tr>
<tr>
<td>SqueezeNet</td>
<td>An image classification model trained on the ImageNet dataset using Caffe</td>
</tr>
<tr>
<td>VGG</td>
<td>An image classification model trained on the ImageNet dataset using Caffe</td>
</tr>
</tbody>
</table>

For more information about Caffe models, see [Caffe Model Zoo](#).

Supporting Caffe Layers

You can use the following Caffe layers to train deep learning models supported by AWS DeepLens.

Supported Caffe Layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BatchNorm</td>
<td>Normalizes the input to have 0-mean and/or unit variance across the batch</td>
</tr>
<tr>
<td>Concat</td>
<td>Concatenates input blobs</td>
</tr>
<tr>
<td>Convolution</td>
<td>Convolves the input with a bank of learned filters</td>
</tr>
<tr>
<td>Deconvolution</td>
<td>Performs in the opposite sensor of the Convolution layer</td>
</tr>
<tr>
<td>Dropout</td>
<td>Performs dropout</td>
</tr>
<tr>
<td>Eltwise</td>
<td>Performs element-wise operations, such as product and sum, along multiple input blobs</td>
</tr>
<tr>
<td>Flatten</td>
<td>Reshapes the input blob into flat vectors</td>
</tr>
<tr>
<td>InnerProduct</td>
<td>Computes an inner product</td>
</tr>
<tr>
<td>Input</td>
<td>Provides input data to the model</td>
</tr>
<tr>
<td>LRN (Local Response Normalization)</td>
<td>Normalizes the input in a local region across or within feature maps</td>
</tr>
<tr>
<td>Permute</td>
<td>Permutes the dimensions of a blob</td>
</tr>
<tr>
<td>Pooling</td>
<td>Pools the input image by taking the max, average, etc., within regions</td>
</tr>
<tr>
<td>Power</td>
<td>Computes the output as ( (\text{shift} + \text{scale} \times x)^{\text{power}} ) for each input element ( x )</td>
</tr>
<tr>
<td>ReLU</td>
<td>Computes rectified linear activations</td>
</tr>
</tbody>
</table>
### Supported Caffe Layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reshape</td>
<td>Changes the dimensions of the input blob, without changing its data</td>
</tr>
<tr>
<td>ROI Pooling</td>
<td>Applies pooling for each region of interest</td>
</tr>
<tr>
<td>Scale</td>
<td>Computes the element-wise product of two input blobs</td>
</tr>
<tr>
<td>Slice</td>
<td>Slices an input layer to multiple output layers along a given dimension</td>
</tr>
<tr>
<td>Softmax</td>
<td>Computes the Softmax activations</td>
</tr>
<tr>
<td>Tile</td>
<td>Copies a blob along specified dimensions</td>
</tr>
</tbody>
</table>

For more information about Caffe layers, see [Caffe Layers](#).
Viewing AWS DeepLens Output Streams

An AWS DeepLens device produces two output streams: the device stream and a project stream. The device stream is an unprocessed video stream. The project stream is the result of the processing that the model performs on the video frames.

You can view the output in a supported web browser when your AWS DeepLens device is online. For more information, see the section called "View Video Stream from AWS DeepLens Device in Browser." (p. 42). In addition, you can also view the output on the device that is connected to a monitor, a keyboard and a mouse. The instructions are given in this section.

Topics

- View Video Streams from AWS DeepLens 2019 Edition(v1.1) Device in Browser (p. 41)
- View Video Streams from AWS DeepLens Device in Browser (p. 42)
- View Video Streams on Your AWS DeepLens Device (p. 44)
- Creating a Lambda Function for Viewing the Project Stream (p. 46)

View Video Streams from AWS DeepLens 2019 Edition(v1.1) Device in Browser

To view project or live streams from the AWS DeepLens 2019 Edition(v1.1) device in a browser, you must have the device’s self-signed streaming certificate downloaded to your computer and then uploaded to a supported browser you'll use. For instructions on how to download the streaming certificate and install it into the browser, see Step 6 of View or Update Your AWS DeepLens 2019 Edition(v1.1) Device Settings (p. 19).

To view video streams from AWS DeepLens 2019 Edition(v1.1) device in a browser

1. Connect the device to your computer with the provided USB cable, if it's not already connected.
2. Do one of the following to launch your devices' AWS DeepLens Stream viewer:
   - Open the device details page on the AWS DeepLens console and choose View video stream under Video streaming to open the stream viewer in a new browser tab.
   - Alternatively, open a new browser tab manually, type https://your-device-ip-address:4000 in the address bar, where your-device-ip-address stands for the IP address of your device (e.g., 192.168.14.78) shown under Device details in the AWS DeepLens console.
3. Because the streaming certificate is self-signed, the browser will display a warning. To accept the warning, follow browser-specific instructions on screen to accept the certificate for the stream viewer to be launched.
   It may take about 30 seconds for the stream viewer to show up.
4. Before any project is deployed, choose Live stream to view live videos from your AWS DeepLens device. After a project is deployed, you can also choose Project stream to view processed videos output from the device.
5. When done with viewing video streams, disconnect the device from your computer to return the computer to its normal network configuration.
View Video Streams from AWS DeepLens Device in Browser

Note
To view a project's output in a supported browser, your device must have the awscam software version 1.3.9 or higher installed. For information to update the device software, see the section called “Update Your Device” (p. 97).

Note
To view a project's output in Chrome on Mac El Capitan or earlier, you must provide a password to load the streaming certificate for viewing the project output. If you have such an old Mac operating system and want to use Chrome, skip the procedure below and follow the instructions in How to View Project Output in the Chrome Browser on Mac El Capitan or Earlier? (p. 118) to set up your browser to view the project output.

To view project output from your AWS DeepLens device in a supported web browser

1. If you have not already downloaded the streaming certificate when registering your device (p. 27) or if you have lost the downloaded copy, do one of the following to download the streaming certificate. The steps are different depending on whether you use the device setup application or not.
   a. Download the streaming certificate without using the device setup page:
      i. Establish an SSH connection to your AWS DeepLens device from your computer:

         ```
         ssh aws_cam@device_local_ip_address
         ```

         An example of `device_local_ip_address` would be `192.168.0.47`. After entering the correct device password, which you specified during the device registration, you're now logged in to the device.

         ii. Make a local copy (`my_streaming_cert.pfx`) of the streaming certificate (`client.pfx`) on the device:

         ```
         sudo cp /opt/awscam/awsmedia/certs/client.pfx /home/aws_cam/
         my_streaming_cert.pfx
         ```

         When prompted, enter the device password to complete the above commands.

         Make sure that the owner of the device-local copy is `aws_cam`.

         ```
         sudo chown aws_cam /home/aws_cam/my_streaming_cert.pfx
         ```

         After this, log out of the device:

         ```
         exit
         ```

         iii. Transfer the copy of the streaming certificate from the device to your computer:

         ```
         scp aws_cam@device_local_ip_address:/home/aws_cam/my_streaming_cert.pfx ~/.Downloads/
         ```

         The example used the Downloads folder under the user's home directory (~/) to transfer the certificate to. You can choose any other writeable directory as the destination folder.
b. Follow the following steps to download the streaming certificate for the AWS DeepLens device:
   
i. Return your device to its setup mode, if necessary, and connect your computer to the
device's ADMC-NNNN Wi-Fi network (p. 23).

   ii. Start the device setup app at http://deeplens.config.

   iii. Follow the on-screen instructions to download the streaming certificate for viewing a
project's output streams.

2. Import into your supported web browser the streaming certificate you downloaded during the
device registration (p. 27).

   a. For Firefox (Windows and macOS Sierra or higher), follow these steps:
      
i. Choose Preferences in Firefox.


   iii. Choose View certificate.

   iv. Choose the Your Certificates tab.

   v. Choose Import.

   vi. Choose the downloaded streaming certificate to load into Firefox.

   vii. When prompted to enter your computer's system password, if your AWS DeepLens
software version is 1.3.23 or higher, type DeepLens in the password input field. If your AWS
DeepLens software version is 1.3.22 or lower, leave the password field blank and follow the
on-screen instruction to finish importing the streaming certificate.

   Note
   Depending on the version of the Firefox you use, you may need to follow steps below,
instead:

   1. From Preferences, choose Advanced.

   2. Choose the Certificates tab.

   3. Choose View Certificates.

   4. On Certificate Manager, choose the Your certificates tab.

   5. Choose Import.

   6. Navigate to and open the downloaded streaming certificate.

   7. When prompted for a password, if your AWS DeepLens software version is 1.3.23 or
higher, type DeepLens in the password input field. If your AWS DeepLens software
version is 1.3.22 or lower, choose OK without entering one.

   b. For Chrome (macOS Sierra or higher), follow these steps:

      i. On your macOS, double-click the downloaded streaming certificate to add it to System
under Keychains and My Certificate under Category.

      Alternatively, open and unlock the Keychain Access app, choose System under Keychains
on the left and My Certificate under Category. Drag and drop the downloaded streaming
certificate into the window.

      ii. Enter your computer's system password.

      iii. On the next screen, if your AWS DeepLens software version is 1.3.23 or higher, type
DeepLens in the password input field. If your AWS DeepLens software version is 1.3.22 or
lower, leave the Password field blank and then choose OK.

   c. For Chrome (Windows and Linux), follow these steps:

      i. In your Chrome browser, open Settings and choose Advanced settings.

      ii. In Privacy and security, choose Manage certificates.
View Video Streams on Your AWS DeepLens Device

In addition to viewing your AWS DeepLens output streams in a browser (p. 42), you can use mplayer to view the streams directly from your AWS DeepLens device after connecting it to a monitor, a keyboard, and a mouse. This is especially useful when your AWS DeepLens device is not online.

Instead of connecting to the device directly using a monitor, a keyboard, and a mouse, you can also use ssh to connect to the device, if SSH access is enabled on the device when it is registered. You can then use mplayer on your work computer to view the streams. Make sure that mplayer is installed on your computer before viewing the output streams from your AWS DeepLens device. For more information about the installation, see mplayer download.

Topics
- View Live Streams on Your AWS DeepLens Device (p. 44)
- View Project Streams on Your AWS DeepLens Device (p. 45)

View Live Streams on Your AWS DeepLens Device

To view an unprocessed device stream on your AWS DeepLens device

1. Plug your AWS DeepLens device into a power outlet and turn it on.
2. Connect a USB mouse and keyboard to your AWS DeepLens.
3. Use the micro HDMI cable to connect your AWS DeepLens to a monitor. A login screen appears on the monitor.
4. Sign in to the device using the SSH password that you set when you registered the device.
5. To see the video stream from your AWS DeepLens, start your terminal and run the following command:
To view a project stream on your AWS DeepLens device

1. Plug your AWS DeepLens device to a power outlet and turn it on.
2. Connect a USB mouse and keyboard to your AWS DeepLens.
3. Use the micro HDMI cable to connect your AWS DeepLens to a monitor. A login screen appears on the monitor.
4. Sign in to the device using the SSH password you set when you registered the device.
5. To see the video stream from your AWS DeepLens, start your terminal and run the following command:

   ```sh
   mplayer -demuxer lavf -lavfdopts format=mjpeg:probesize=32 /tmp/results.mjpeg
   ```

6. To stop viewing the video stream and end your terminal session, press Ctrl+C.
Creating a Lambda Function for Viewing the Project Stream

To view the project stream, you need an AWS Lambda function that interacts with the mjpeg stream on your device and the deep learning model. For the sample projects included with AWS DeepLens, the code is included in the inference Lambda function for the project. For your custom projects, you need to create a Lambda function that performs this task.

Create a Lambda function for your custom projects

Add the following sample code to your projects and change the model name and the dimensions as appropriate. https://docs.aws.amazon.com/deeplens/latest/dg/

```python
import os
import greengrasssdk
from threading import Timer
import time
import awscam
import cv2

# Create an AWS Greengrass core SDK client.
client = greengrasssdk.client('iot-data')

# The information exchanged between AWS IoT and the AWS Cloud has
# a topic and a message body.
# This is the topic that this code uses to send messages to the Cloud.
iotTopic = '${aws/things/{}/infer'.format(os.environ['AWS_IOT_THING_NAME'])
_, frame = awscam.getLastFrame()
_, jpeg = cv2.imencode('.jpg', frame)

class FIFO_Thread(Thread):
    def __init__(self):
        ''' Constructor. '''
        Thread.__init__(self)

    def run(self):
        fifo_path = '/tmp/results.mjpeg'
        if not os.path.exists(fifo_path):
            os.mkfifo(fifo_path)
        f = open(fifo_path, 'w')
        client.publish(topic=iotTopic, payload="Opened Pipe")
        while Write_To_FIFO:
            try:
                f.write(jpeg.tobytes())
            except IOError as e:
                continue

def greengrass_infinite_infer_run():
    try:
        modelPath = '/opt/awscam/artifacts/mxnet_deploy_ssd_resnet50_300_FP16_FUSED.xml'
        modelType = "ssd"
        input_width = 300
        input_height = 300
        max_threshold = 0.25
                  15: 'person', 16: 'pottedplant', 17: 'sheep',
                  18: 'sofa', 19: 'train', 20: 'tvmonitor'})
    ```
results_thread = FIFO_Thread()
results_thread.start()

# Send a starting message to the AWS IoT console.
client.publish(topic=iotTopic, payload="Object detection starts now")

# Load the model to the GPU (use {"GPU": 0} for CPU).
mcfg = {"GPU": 1}
model = awscam.Model(modelPath, mcfg)
client.publish(topic=iotTopic, payload="Model loaded")

ret, frame = awscam.getLastFrame()
if ret == False:
    raise Exception("Failed to get frame from the stream")

yscale = float(frame.shape[0]/input_height)
xscale = float(frame.shape[1]/input_width)

doInfer = True
while doInfer:
    # Get a frame from the video stream.
    ret, frame = awscam.getLastFrame()

    # If you fail to get a frame, raise an exception.
    if ret == False:
        raise Exception("Failed to get frame from the stream")

    # Resize the frame to meet the model input requirement.
    frameResize = cv2.resize(frame, (input_width, input_height))

    # Run model inference on the resized frame.
    inferOutput = model.doInference(frameResize)

    # Output the result of inference to the fifo file so it can be viewed with mplayer.
    parsed_results = model.parseResult(modelType, inferOutput)['ssd']
    label = '{
        for obj in parsed_results:
            if obj['prob'] > max_threshold:
                xmin = int( xscale * obj['xmin'] ) + int((obj['xmin'] - input_width/2) + input_width/2)
                ymin = int( yscale * obj['ymin'] )
                xmax = int( xscale * obj['xmax'] ) + int((obj['xmax'] - input_width/2) + input_width/2)
                ymax = int( yscale * obj['ymax'] )
                cv2.rectangle(frame, (xmin, ymin), (xmax, ymax), (255, 165, 20), 4)
                label += '"{}": {:.2f},'.format(outMap[obj['label']], obj['prob'])
                label_show = '{}:    {:.2f}%'.format(outMap[obj['label']], obj['prob']*100)
                cv2.putText(frame, label_show, (xmin, ymin-15), cv2.FONT_HERSHEY_SIMPLEX, 0.5, (255, 165, 20), 4)
            label += 'null': 0.0}

e except Exception as e:
    msg = "Test failed: " + str(e)
    client.publish(topic=iotTopic, payload=msg)

    # Asynchronously schedule this function to be run again in 15 seconds.
    Timer(15, greengrass_infinite_infer_run).start()

    # Execute the function.
    greengrass_infinite_infer_run()
# This is a dummy handler and will not be invoked. 
# Instead, the code is executed in an infinite loop for our example.
def function_handler(event, context):
    return

After you've created and deployed the Lambda function, follow the instructions in the section called "View Video Stream from AWS DeepLens Device in Browser." (p. 42) or View Project Streams on Your AWS DeepLens Device (p. 45) to view the processed project stream.
Working with AWS DeepLens Sample Projects

When your AWS DeepLens device is registered and connected to the AWS Cloud, you're ready to create an AWS DeepLens project and deploy it to the device to run computer vision application on. An AWS DeepLens project is made up of an AWS DeepLens model and the associated AWS Lambda function to run inference with. You can use a pre-trained model in your project or you can train a custom model.

AWS DeepLens provides several sample projects for you to deploy and run inference on right out of the box. Here, you'll learn how to use a sample project and deploy it to your AWS DeepLens device. Before we start, let's get an overview of the sample projects.

Topics
- AWS DeepLens Sample Projects Overview (p. 49)
- Create and Deploy an AWS DeepLens Sample Project in the AWS DeepLens Console (p. 51)
- Relay an AWS DeepLens Project Output through AWS SMS (p. 53)
- Use SageMaker to Provision a Pre-trained Model for a Sample Project (p. 59)

AWS DeepLens Sample Projects Overview

To get started with AWS DeepLens, use the sample project templates. AWS DeepLens sample projects are projects where the model is pre-trained so that all you have to do is create the project, import the model, deploy the project, and run the project. Other sections in this guide teach you to extend a sample project's functionality so that it performs a specified task in response to an event, and train a sample project to do something different than the original sample.

Artistic Style Transfer

This project transfers the style of an image, such as a painting, to an entire video sequence captured by AWS DeepLens.

This project shows how a Convolutional Neural Network (CNN) can apply the style of a painting to your surroundings as it's streamed with your AWS DeepLens device. The project uses a pretrained optimized model that is ready to be deployed to your AWS DeepLens device. After deploying it, you can watch the stylized video stream.

You can also use your own image. After fine tuning the model for the image, you can watch as the CNN applies the image's style to your video stream.

- Project model: deeplens-artistic-style-transfer
- Project function: deeplens-artistic-style-transfer

Object Recognition

This project shows you how a deep learning model can detect and recognize objects in a room.

The project uses the Single Shot MultiBox Detector (SSD) framework to detect objects with a pretrained resnet_50 network. The network has been trained on the Pascal VOC dataset and is capable of recognizing 20 different kinds of objects. The model takes the video stream from your AWS DeepLens device as input and labels the objects that it identifies. The project uses a pretrained optimized model that is ready to be deployed to your AWS DeepLens device. After deploying it, you can watch your AWS DeepLens model recognize objects around you.

Note
When deploying an SageMaker-trained SSD model, you must first run deploy.py (available from https://github.com/apache/incubator-mxnet/tree/v1.x/example/ssd/) to convert the
model artifact into a deployable model. After cloning or downloading the MXNet repository, run the `git reset --hard 73d88974f8bca1e68441606fb0787a2cd17eb364` command before calling `deploy.py` to convert the model, if the latest version does not work.

The model is able to recognize the following objects: airplane, bicycle, bird, boat, bottle, bus, car, cat, chair, cow, dining table, dog, horse, motorbike, person, potted plant, sheep, sofa, train, and TV monitor.

- **Project model**: deeplens-object-detection
- **Project function**: deeplens-object-detection

## Face Detection and Recognition

With this project, you use a face detection model and your AWS DeepLens device to detect the faces of people in a room.

The model takes the video stream from your AWS DeepLens device as input and marks the images of faces that it detects. The project uses a pretrained optimized model that is ready to be deployed to your AWS DeepLens device.

- **Project model**: deeplens-face-detection
- **Project function**: deeplens-face-detection

## Hot Dog Recognition

Inspired by a popular television show, this project classifies food as either a hot dog or not a hot dog.

It uses a model based on the SqueezeNet deep neural network. The model takes the video stream from your AWS DeepLens device as input, and labels images as a hot dog or not a hot dog. The project uses a pretrained, optimized model that is ready to be deployed to your AWS DeepLens device. After deploying the model, you can use the Live View feature to watch as the model recognizes hot dogs.

You can edit this model by creating Lambda functions that are triggered by the model's output. For example, if the model detects a hot dog, a Lambda function could send you an SMS message. To learn how to create this Lambda function, see [Use SageMaker to Provision a Pre-trained Model for a Sample Project](p. 59)

## Cat and Dog Recognition

This project shows how you can use deep learning to recognize a cat or a dog.

It is based on a convolutional neural network (CNN) architecture and uses a pretrained Resnet-152 topology to classify an image as a cat or a dog. The project uses a pretrained, optimized model that is ready to be deployed to your AWS DeepLens device. After deploying it, you can watch as AWS DeepLens uses the model to recognize your pets.

- **Project model**: deeplens-cat-and-dog-recognition
- **Project function**: deeplens-cat-and-dog-recognition

## Action Recognition

This project recognizes more than 30 kinds of activities.

It uses the Apache MXNet framework to transfer learning from a SqueezeNet trained with ImageNet to a new task. The network has been tuned on a subset of the UCF101 dataset and is capable of recognizing more than 30 different activities. The model takes the video stream from your AWS DeepLens device.
as input and labels the actions that it identifies. The project uses a pretrained, optimized model that is ready to be deployed to your AWS DeepLens device.

After deploying the model, you can watch your AWS DeepLens use the model to recognize 37 different activities, such as applying makeup, applying lipstick, participating in archery, playing basketball, bench pressing, biking, playing billiards, blowing drying your hair, blowing out candles, bowling, brushing teeth, cutting things in the kitchen, playing a drum, getting a haircut, hammering, handstand walking, getting a head massage, horseback riding, hula hooping, juggling, jumping rope, doing jumping jacks, doing lunges, using nunchucks, playing a cello, playing a flute, playing a guitar, playing a piano, playing a sitar, playing a violin, doing pushups, shaving, skiing, typing, walking a dog, writing on a board, and playing with a yo-yo.

- **Project model**: deepdens-action-recognition
- **Project function**: deepdens-action-recognition

### Head Pose Detection

This sample project uses a deep learning model generated with the TensorFlow framework to accurately detect the orientation of a person's head.

This project uses the ResNet-50 network architecture to detect the orientation of the head. The network has been trained on the Prima HeadPose dataset, which comprises 2,790 images of the faces of 15 people, with variations of pan and tilt angles from -90 to +90 degrees. We categorized these head pose angles to 9 head pose classes: down right, right, up right, down, middle, up, down left, left, and up left.

To help you get started, we have provided a pretrained, optimized model ready to deploy to your AWS DeepLens device. After deploying the model, you can watch AWS DeepLens recognize various head poses.

- **Project model**: deepdens-head-pose-detection
- **Project function**: deepdens-head-pose-detection

### Bird Classification

This project makes prediction of the top 5 bird species from a static bird photo captured by the AWS DeepLens camera.

This project uses the ResNet-18 neural network architecture to train the model with the CUB-200 dataset. The trained model can identify 200 different bird species. Because the number of categories are large, the project outputs only the top 5 most probable inference results. To reduce the background noise for improved precision, a cropped zone located at the middle of the camera image is used for inference. You can view the cropped zone from the project video streaming. By positioning the static bird photo in the box zone, inference results are illustrated on top left of the project view.

- **Project model**: deepdens-bird-detection
- **Project function**: deepdens-bird-detection

### Create and Deploy an AWS DeepLens Sample Project in the AWS DeepLens Console

In this walkthrough, you’ll use the AWS DeepLens console to create an AWS DeepLens project from the [Object Detection sample project template](#) to create an AWS DeepLens project. The pre-trained object detection model can analyze images from a video stream captured on your AWS DeepLens device.
and identify an objects as one of as many as 20 labeled image types. The instructions presented here apply to creating and deploying other AWS DeepLens sample project.

When creating a sample project, the fields in the console are pre-populated for you so you can accept the defaults. In the Project content portion of the screen, you need to know the project's model and inference function. You can find the information for the individual projects in AWS DeepLens Sample Projects Overview (p. 49).

The following diagram presents a high-level overview of the processes to use the AWS DeepLens console to create and deploy a sample project.

Create and Deploy Your Project

Follow the steps below to create and deploy the Object Detection sample project.

To create and deploy an AWS DeepLens sample project using the AWS DeepLens console

2. Choose Projects, then choose Create new project.
3. On the Choose project type screen
   a. Choose Use a project template, then choose the sample project you want to create. For this exercise, choose Object detection.
   b. Scroll to the bottom of the screen, then choose Next.
4. On the Specify project details screen
   a. In the Project information section:
      i. Either accept the default name for the project, or type a name you prefer.
      ii. Either accept the default description for the project, or type a description you prefer.
   b. Choose Create.

   This returns you to the Projects screen where the project you just created is listed with your other projects.
5. On the Projects screen, choose the radio button to the left of your project name or choose the project to open the project details page, then choose Deploy to device.

6. On the Target device screen, from the list of AWS DeepLens devices, choose the radio button to the left of the device that you want to deploy this project to. An AWS DeepLens device can have only one project deployed to it at a time.

7. Choose Review.

If a project is already deployed to the device, you will see an error message that deploying this project will overwrite the project that is already running on the device. Choose Continue project.

This will take you to the Review and deploy screen.

8. On the Review and deploy screen, review your project and choose either Previous to go back and make changes, or Deploy to deploy the project.

Important
Deploying a project incurs costs for the AWS services that are used to run the project.

For instructions on viewing your project's output, see Viewing AWS DeepLens Output Streams (p. 41).

Relay an AWS DeepLens Project Output through AWS SMS

In this section, you take the "Hotdog recognition" sample project and add some rule-based functionality to it to make AWS DeepLens send an SMS notification whenever it detects a hot dog. Though we use the "Hotdog recognition" sample project in this topic, this process could be used for any project, sample or custom.

This section demonstrates how to extend your AWS DeepLens projects to interact with other AWS services. For example, you could extend AWS DeepLens to create:

- A dashboard and search interface for all objects and faces detected by AWS DeepLens with timelines and frames using Amazon OpenSearch Service.
- Anomaly detection models to detect the number of people walking in front of your store using Managed Service for Apache Flink.
- A face detection and celebrity recognition application to identity VIPs around you using Amazon Rekognition.

In this exercise, you modify the project you previously created and edited (see Use SageMaker to Provision a Pre-trained Model for a Sample Project (p. 59)) to use the AWS IoT rules engine and an AWS Lambda function.

Topics
- Create and Configure the Lambda Function (p. 53)
- Disable the AWS IoT Rule (p. 58)

Create and Configure the Lambda Function

Create and configure an AWS Lambda function that runs in the Cloud and filters the messages from your AWS DeepLens device for those that have a high enough probability (>0.5) of being a hot dog. You can also change the probability threshold.
Create a Lambda Function

1. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/. Make sure you have selected the US East (N. Virginia) AWS Region.
2. Choose Create function.
3. Choose Author from scratch.
4. Type a name for the Lambda function, for example, `<your name>_hotdog_notifier`.
5. For Permissions, choose the Create a new Role from AWS policy templates under Execution role.
6. Type a name for the role; for example, `<your name>_hotdog_notifier`.
7. For Policy Templates, choose SNS Publish policy and AWS IoT Button permissions.
Basic information

Function name
Enter a name that describes the purpose of your function.
mytest-hotdog-notifier
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime
Choose the language to use to write your function.
Node.js 10.x

Permissions
Lambda will create an execution role with permission to upload logs to Amazon CloudWatch Logs. You can configure and

Choose or create an execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
Create a new role from AWS policy templates

Role creation might take a few minutes. The new role will be scoped to the current function. To use

Role name
Enter a name for your new role.
mytest-hotdog-notifier-role
Use only letters, numbers, hyphens, or underscores with no spaces.

Policy templates
Choose one or more policy templates.

AWS IoT Button permissions
SNS
Amazon SNS publish policy
SNS
8. Choose **Create function**.

### Add an AWS IoT Rule

After the Lambda function is created successfully, you need to set up an AWS IoT rule to trigger the action you specify in your Lambda function (the next step) when an event occurs in the data source. To set up the rule, follow the steps below to add an AWS IoT trigger to the function.

1. Choose **+ Add trigger**. You may need to expand the **Design** section in the Lambda console, if it's not already expanded.
2. Choose **AWS IoT** under **Trigger configuration**.
3. For **IoT type**, choose **Custom IoT rule**.
4. For **Rule**, choose **Create a new rule**.
5. For **Rule name**, type a name (**<your-name>_search_hotdogs**).
6. Optionally, give a description for the rule under **Rule description**.
7. Under **Rule query statement**, type into the box an AWS IoT topic query statement of the following format, replacing the red text with the AWS IoT topic for your AWS DeepLens.

   ```
   Select Hotdog from '/$aws/deeplens/$aws/things/deeplens_5e6d406g-2bf4-4444-9d4f-4668f7366855/infer'
   ```

   This query captures messages from your AWS DeepLens in JSON format:
   ```
   { "Hotdog" : "0.5438" }
   ```

   To find the AWS IoT topic for your AWS DeepLens, navigate to **Devices** on your AWS DeepLens, choose your device, then scroll to the bottom of the device detail page.

8. Toggle on the **Enable trigger** option.
9. Choose **Add** to finish creating the AWS IoT rule.

### Configure the Lambda Function

Configure the Lambda function by replacing the default code with custom code and adding an environmental variable. For this project, you also need to modify the custom code that we provide.

1. In AWS Lambda, choose **Functions**, then choose the name of your function.
2. On the **your-name_hotdog_notifier** page, choose **Configuration**.
3. In the function code box, delete all of the code.
4. Paste the following JavaScript code in the function code box. You need to change one line in the code to indicate how you want to get notifications. You do that in the next step.

   ```javascript
   /**
   * This is a sample Lambda function that sends an SMS notification when your
   * AWS DeepLens device detects a hot dog.
   * Follow these steps to complete the configuration of your function:
   * Update the phone number environment variable with your phone number.
   */
   const AWS = require('aws-sdk');
   ```
const email = process.env.email;
const phone_number = process.env.phone_number;
const SNS = new AWS.SNS({ apiVersion: '2010-03-31' });

exports.handler = (event, context, callback) => {
  console.log('Received event:', event);
  // publish message
  const params = {
    Message: 'Your AWS DeepLens device just identified a hot dog. Congratulations!',
    PhoneNumber: phone_number
  };
  if (event.Hotdog > 0.5) {
    SNS.publish(params, callback);
  }
};

5. Add one of the following lines of code in the location indicated in the code block. In the next step, you add an environmental variable that corresponds to the code change you make here.

- To receive email notifications: `const email=process.env.email;`
- To receive phone notifications: `const phone_number=process.env.phone_number;`

6. Choose Environmental variables and add one of the following:

<table>
<thead>
<tr>
<th>Notification by</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>email</td>
<td>Your complete email address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>YourAlias@ISP.com</code></td>
</tr>
<tr>
<td>Phone</td>
<td>phone_number</td>
<td>Your phone number with country code.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>US +1 8005551212</code></td>
</tr>
</tbody>
</table>

The key value must match the const name in the line of code that you added in the previous step.

7. Choose Save and Test (on the upper right).

**Test Your Configuration**

**To test your configuration**

2. Choose Test.
3. Publish the following message to the topic that you defined in your rule: `{ "Hotdog" : "0.6382" }.

   You should receive the SMS message that you defined in your Lambda function: Your AWS DeepLens device just identified a hot dog. Congratulations!

**Test Using the Hot Dog Project**

If you haven't already deployed the Hot Dog project, do the following.
1. Navigate to https://console.aws.amazon.com/deeplens/home?region=us-east-1#firstrun/ and choose Projects/Create a project template/Hotdog or Not Hotdog.
2. Deploy the project to your device. 
   For more information, see Create and Deploy an AWS DeepLens Sample Project in the AWS DeepLens Console (p. 51).
3. Show your AWS DeepLens a hot dog to see if it detects it and sends you the confirmation message.

To experiment, change the probability threshold for triggering the Lambda function and see what happens.

**Disable the AWS IoT Rule**

Unless you want AWS DeepLens to keep notifying you when it sees a hot dog, disable the AWS IoT rule.

2. Choose Act, then choose the rule that you created for this exercise, <your-name>_search_hotdogs.
3. In the upper-right corner, choose Actions, then choose Disable.
Use SageMaker to Provision a Pre-trained Model for a Sample Project

In this example, you start with a SqueezeNet object detection model and use SageMaker to train it to perform binary classification to determine whether an object is a hot dog. The example shows you how to edit a model to perform binary classification, and explains learning rate and epochs. We have provided a Jupyter notebook instance, which is open source software for interactive computing. It includes the editing code to execute and explanations for the entire process.

After training the model, you import its artifacts into AWS DeepLens, and create a project. You then watch as your AWS DeepLens detects and identifies hot dogs.

Topics
- **Step 1: Create an Amazon S3 Bucket** (p. 60)
- **Step 2: Create an SageMaker Notebook Instance** (p. 61)
- **Step 3: Edit the Model in SageMaker** (p. 62)
- **Step 4: Optimize the Model** (p. 63)
- **Step 5: Import the Model** (p. 64)
- **Step 6: Create an Inference Lambda Function** (p. 65)
- **Step 7: Create a New AWS DeepLens Project** (p. 66)
- **Step 8: Review and Deploy the Project** (p. 67)
- **Step 9: View Your Model's Output** (p. 68)
Step 1: Create an Amazon S3 Bucket

Before you begin, be sure that you have created an AWS account, and the required IAM users and roles.

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose Create bucket.
3. On the Name and region tab:
   a. Name the bucket deeplens-sagemaker-<some_string>, where <some_string> can be any string to make the bucket name unique across AWS. An example would be your account name or ID.
   
   **Note**
   The bucket name must begin with `deeplens-sagemaker-` to work with the default access policies. Otherwise, the services will not be able to access it.

   b. Verify that you are in the US East (N. Virginia) region.
   c. Choose Next.
4. On the Configure options tab, choose Next.
5. On the Set permissions tab, choose Grant Amazon S3 Log Delivery group write access to this bucket from the Manage system permissions drop-down menu, then choose Next.
6. On the Review tab, review your settings then choose Create bucket.
7. On the created bucket's page, choose the Overview tab and then choose Create folder.
8. Name the folder test then choose Save.

   To use the folder with the example notebook instance to be created next, you must name the folder as `test`, unless you change the default folder name in the notebook.
Step 2: Create an SageMaker Notebook Instance

Create an SageMaker notebook instance.

1. Open the Amazon SageMaker console at https://console.aws.amazon.com/sagemaker/.
   Make sure that you have chosen the us-east-1 — US East (N. Virginia) Region.
2. Choose Notebook instances from the navigation pane and then choose Create notebook instance.
3. On the Create notebook instance page, then do the following:
   a. Under Notebook instance settings, type a name for the notebook in the Notebook instance name input field; for example, <your-name>-hotdog.
   b. For Notebook instance type, choose ml.t2.medium.
   c. For Permissions and encryption, under IAM role, choose Create a new role, if this is the first time you run a notebook, type deeplens-sagemaker in the Specific S3 buckets input field, and then choose Create role.

After you've created the first notebook instance for AWS DeepLens, you can choose an available IAM role from the Use existing role list.

If you've already created the AWSDeepLensSageMaker role as part of the setup, choose Enter a custom IAM role ARN, paste the Amazon Resource Name (ARN) of your SageMaker role in the Custom IAM role ARN box. You can find the ARN of your SageMaker role as follows:

   i. Open the IAM console at https://console.aws.amazon.com/iam/.
   ii. In the navigation pane, choose Roles.
   iii. Find the AWSDeepLensSagemakerRole and choose its name. This takes you to the role's Summary page.
   iv. On the Summary page, locate and copy the Role ARN. The ARN will look something like this:

```
arn:aws:iam::<account id>:role/AWSDeepLensSagemakerRole
```

   d. All other settings are optional. Skip them for this exercise.

   Tip
   If you want to access resources in your VPC from the notebook instance, choose a VPC and a SubnetId. For Security Group, choose the default security group of the VPC. The inbound and outbound rules of the default security group are sufficient for the exercises in this guide.

   e. Choose Create notebookinstance.

Your new notebook instance is now available on the Notebooks page.
Step 3: Edit the Model in SageMaker

In this step, you open the `<your-name>-hotdog` notebook and edit the object detection model so it recognizes a hot dog. The notebook contains explanations to help you through each step.

1. Open the Amazon SageMaker console at https://console.aws.amazon.com/sagemaker/.
2. Make sure the US East (N. Virginia) Region is chosen.
3. In the navigation pane, choose Notebook instances.
4. On the Notebooks page, choose the radio button to the left of the notebook instance that you just created (`<your-name>-hotdog`). When the notebook's status is InService, choose Open Jupiter.
6. Download the .zip file or clone the Git repository with the following command. If you downloaded the .zip file, locate it and extract all.

```
git clone git@github.com:aws-samples/reinvent-2017-deeplens-workshop.git
```

If you downloaded the .zip file, locate it and extract all.

You now upload the training file and use it to edit the model.

1. On the Jupyter tab, choose Upload.
2. Navigate to the extracted file `deeplens-hotdog-or-not-hotdog.ipynb` then choose Open, then choose Upload.
3. Locate and choose the `deeplens-hotdog-or-not-hotdog` notebook.
4. In the upper right corner of the Jupyter screen, verify that the kernel is `conda_mxnet_p36`. If it isn't, change the kernel.
5. In the `deeplens-hotdog-or-not-hotdog.ipynb` file, search for `bucket= 'your S3 bucket name here'`. Replace `your s3 bucket name here` with the name of your S3 bucket, for example `deeplens-sagemaker-<your-name>`.

Return to the top of the file.

For each step (In [#]:) in the file:

a. Read the step's description.

b. If the block has code in it, place your cursor in the code block and run the code block. To run a code block in Jupyter, use `Ctrl+<Enter>` or choose the run icon ( ).

Important

Each step is numbered in a fashion such as In [1]:. While the block is executing, that changes to In [*]:. When the block finishes executing it returns to In [1]:. Do not move on to the next code block while the current block is still running.

6. After you finish editing the model, return to the Amazon S3 console, choose your bucket name, choose the test folder, and then verify that the following artifacts of the edited model are stored in your S3 bucket's test folder.

- Hotdog_or_not_model-0000.params
- Hotdog_or_not_model-symbol.json
Step 4: Optimize the Model

Now that you have a trained mxNet model there is one final step that is required before you run the model on the AWS DeepLens's GPU. The trained mxNet model does not come in a computationally optimized format. If we deploy the model in the original format it will run on the CPU via mxNet at sub optimal speed. In order to run the model at optimal speed on the GPU we need to perform model optimization. For instructions on how to optimize your MXNet model, see Optimize a Custom Model (p. 71).
Step 5: Import the Model

Import the edited model into AWS DeepLens.

2. Choose Models, then choose Import model.
3. For Import model to AWS DeepLens, choose Externally trained model.
4. For Model settings, do the following:
   a. For Model artifact, type the path to the artifacts that you uploaded to the Amazon S3 bucket in the previous step. The path begins with s3://deeplens-. For example, if you followed the naming in Step 1, the path will be s3://deeplens-sagemaker-<your-name>/<dir>.
   b. For Model name, type a name for the model.
   c. For Model description, type a description.
5. Choose Import model.
Step 6: Create an Inference Lambda Function

Use the AWS Lambda console to create a Lambda function that uses your model. For specific instructions with sample code, see Create and Publish an AWS DeepLens Inference Lambda Function (p. 71).
Step 7: Create a New AWS DeepLens Project

Now create a new AWS DeepLens project and add the edited model to it.

2. Choose Projects.
3. Choose Create new project.
4. For Choose project type, choose Create a new blank project, then choose Next.
5. For Project information, type a name and description for this project.
6. For Project content, choose Add model.
7. Search for and choose the model that you just created, then choose Add model.
8. Choose Add function, then choose, for example, deeplens-hotdog-no-hotdog, then choose Add function.
9. Choose Create.
Step 8: Review and Deploy the Project

2. From the list of projects, choose the project that you just created, then choose Deploy to device.
3. Choose your AWS DeepLens as your target device, then choose Review.
4. Review the settings, then choose Deploy.

**Important**

Deploying a project incurs costs for the various AWS services that are used.
Step 9: View Your Model's Output

To view your model's output, follow the instructions at Viewing AWS DeepLens Output Streams (p. 41).
Working with AWS DeepLens Custom Projects

After you've explored one or more sample projects, you may want to create and deploy your own AWS DeepLens projects. It means that you'll need to do all or most of the following.

• Train a custom deep learning model either in SageMaker or elsewhere.
• Import the model into AWS DeepLens.
• Create and publish an inference function.
• Create a AWS DeepLens project and add the model and the inference function to it.
• Deploy the project to your AWS DeepLens device.

We'll walk you through these tasks in this section.

Topics

• Import Your SageMaker Trained Model (p. 69)
• Import an Externally Trained Model (p. 69)
• Optimize a Custom Model (p. 71)
• Create and Publish an AWS DeepLens Inference Lambda Function (p. 71)
• Create and Deploy a Custom AWS DeepLens Project (p. 75)
• Use SageMaker Neo to Optimize Inference on AWS DeepLens (p. 76)

Import Your SageMaker Trained Model

To use your SageMaker trained model for your computer vision application, you must import it into AWS DeepLens.

To import your SageMaker trained model into AWS DeepLens

2. From the navigation pane, choose Models then choose Import model.
3. For Import source choose SageMaker trained model.
4. In the Model settings area:
   a. From the list of completed jobs, choose the SageMaker training job ID for the model you want to import.

       The ID of the job must begin with deeplens-, unless you've customized the AWSDeepLensServiceRolePolicy (used for registering the device) to extend the policy to allow AWS DeepLens to access SageMaker's training jobs not starting with deeplens*.

       If you do not find the job you're looking for in the list, go to the SageMaker console and check the status of the jobs to verify that it has successfully completed.
   b. For the Model name, type the name you want for the model. Model names can contain alphanumeric characters and hypens, and be no longer than 100 characters.
   c. For the Description you can optionally type in a description for your model.
   d. Choose Import model.

Import an Externally Trained Model

To use an externally trained model, import it.
To import an externally trained model

2. In the navigation pane, choose Models, then choose Import model.
3. For Import source, choose Externally trained model.
4. For Model settings, provide the following information.
   a. For Model artifact path, type the full path to the Amazon Simple Storage Service (Amazon S3) location of the artifacts created when you trained your model. The path begins with `s3://deeplens-`. For example, if you followed the naming conventions we use throughout this documentation, the path will be `s3://deeplens-sagemaker-your_name/<dir>`.
   b. For Model name, type a name. A model name can have a maximum of 100 alphanumeric characters and hypens.
   c. Optional. For Description, type a description of the model.
   d. Choose Import model.
Optimize a Custom Model

AWS DeepLens uses the Computer Library for Deep Neural Networks (cDNN) to leverage the GPU for performing inferences. If your model artifacts are not compatible with the cDNN format, you must convert your model artifacts by calling the model optimization (mo) module. The process is known as model optimization. Model artifacts output by MXNet, Caffe or TensorFlow are not optimized.

To optimize your model artifacts, call the `mo.optimize` method as illustrated in the following code:

```python
error, model_path = mo.optimize(model_name, input_width, input_height)
```

To load a model artifact for inference in your inference Lambda function, specify the model artifact path on the device. For an unoptimized model artifact, you must use the `model_path` returned from the above method call.

Models are deployed to the `/opt/awscam/artifacts` directory on the device. An optimized model artifact is serialized into an XML file and you can assign the file path directly to the `model_path` variable. For an example, see the section called “Create and Publish an Inference Lambda Function” (p. 71).

For MXNet model artifacts, the model optimizer can convert `.json` and `.params` files. For Caffe model artifacts, the model optimizer can take `.prototxt` or `.caffemodel` files. For TensorFlow model artifacts, the model optimizer expects the frozen graph (.pb) file.

For more information about the model optimizer, see `Model Optimization (mo) Module` (p. 130).

Create and Publish an AWS DeepLens Inference Lambda Function

This topic explains how to add an AWS Lambda inference function to your custom AWS DeepLens project. Inference is the step where the model is shown images it has never seen before and asked to make a prediction. The inference function optimizes the model to run on AWS DeepLens and feeds each camera frame into the model to get predictions. For the inference function, you use AWS Lambda to create a function that you deploy to AWS DeepLens. The inference function runs locally on the AWS DeepLens device over each frame that comes out of the camera.

AWS DeepLens supports Lambda inference functions written in Python 2.7 and Python 3.7. Python 3.7 requires requires device software v1.4.5. You will write the Lambda function in the browser and then deploy it to run on AWS DeepLens.

**To create and publish an inference Lambda function for your AWS DeepLens project**

1. Download the [AWS DeepLens inference function template](#) to your computer. Do not unzip the downloaded file.

   The zip file contains the following:
   - `lambda_function.py` — this file contains the Lambda function. AWS DeepLens will run this file after your AWS DeepLens project has been deployed.
   - `local_display.py` — this file contains a helper class to write the modified frames from the camera into the project video stream.
   - `greengrasssdk` — this folder contains the AWS IoT Greengrass SDK. It is used to send prediction results back to the cloud or to another IoT device.
You will be modifying lambda_function.py to pull frames from the camera, perform inference, and send predictions back through AWS IoT Greengrass.

2. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/.

3. Choose Create function, then choose Author from Scratch.

4. In the Basic information section:
   a. Under Function name, type a name for your Lambda function, for example, deeplens-object-detection.

   The function name must start with deeplens.
   b. Under Runtime, choose Python 2.7 or Python 3.7.
   c. Under Permissions, expand Choose or create an execution role, if it's not already expanded.
   d. Under Execution role, choose Use an existing role.
   e. From the Existing role dropdown list, choose service-role/AWSDeepLensLambdaRole, which was created when you registered your device.

5. Scroll to the bottom of the page and choose Create function.

6. In the Function code section, do the following:
   b. Under Function package, choose Upload, and then select deeplens_inference_function_template.zip.

7. Choose Save (on the upper-right corner of the Lambda console) to load the basic Lambda function into the code editor.

8. In the Lambda code editor, open lambda_function.py:

   **Preserve import dependency**
   The cv2 library has a dependency on the awscam module. If you modify the lambda_function.py template, be sure that it continues to import the awscam module before the cv2 library.

   ```python
   import json
   import awscam
   import mo
   import cv2
   import greengrasssdk
   import os
   from local_display import LocalDisplay

   def lambda_handler(event, context):
     """Empty entry point to the Lambda function invoked from the edge."""
     return

   def infinite_infer_run():
     """Run the DeepLens inference loop frame by frame""
     # Load the model here
     while True:
       # Get a frame from the video stream
       ret, frame = awscam.getLastFrame()
       # Do inference with the model here
       # Send results back to IoT or output to video stream
       infinite_infer_run()
   ```

   Let's examine this code line by line.
The `json` module lets your Lambda function work with JSON data and send results back through AWS IoT.

The `awscam` module allows your Lambda function to use the [AWS DeepLens device library](p. 124) to grab camera frames, perform inference with an optimized model and parse inference results. For more information, see [Model Object](p. 125).

The `mo` module allows your Lambda function to access the AWS DeepLens model optimizer. It optimizes the model trained in the cloud to run efficiently on the DeepLens GPU. For more information, see [Model Optimization (mo) Module](p. 130).

The `cv2` module lets your Lambda function access the Open CV library used for image preprocessing.

The `greengrasssdk` module exposes the AWS IoT Greengrass API for the Lambda function to send messages to the AWS Cloud, including sending operational status and inference results to AWS IoT.

The `local_display` file contains a helper class to write to the project video stream. This helps you draw bounding boxes or text directly onto the DeepLens video stream.

The `lambda_handler` is typically where you put the code for Lambda functions that are invoked once and then stopped. We want the Lambda function on AWS DeepLens to run and process frames continuously. We will leave `lambda_handler` empty and define another function `infinite_infer_run` that can run forever.

The `infinite_infer_run` function contains a while loop that runs forever. It pulls uses `awscam.getLastFrame` to pull frames from the camera on each iteration.

9. In this step, you add code to load the inference model and pass the camera frame to it to get predictions. For this example, we assume that you have trained a model to differentiate between a dog and a cat.

In the Lambda code editor, under the comment `# Load the model here`, add the following:

```python
# Model details
input_width = 224
input_height = 224
model_name = 'image-classification'
model_type = 'classification'
output_map = {0: 'dog', 1: 'cat'}

# Optimize the model
error, model_path = mo.optimize(model_name,input_width,input_height)

# Load the model onto the GPU.
model = awscam.Model(model_path, {'GPU': 1})
```

AWS DeepLens uses the Intel OpenVino model optimizer to optimize the model trained in the cloud. `model_name` is the name of the model file you want to load. For models trained with Amazon SageMaker, the model typically has 2 files: a `<model_name>-symbol.json` file and a `<model_name>-###.params` file.

`input_width` and `input_height` refer to the size of the images used to train your network. During inference, the same-sized image is passed in.

`model_type` will tell the `awscam` package how to parse the results. Other model types include `ssd` (single shot detector) and `segmentation`.

`output_map` helps turn the integer results from the model back to human-readable labels.

10. In this step, you add code to pass camera frames through the model to get predictions.
In the Lambda code editor, under the comment # Do inference with the model here, add the following:

```python
frame_resize = cv2.resize(frame, (input_height, input_width))
predictions = model.doInference(frame_resize)
parsed_inference_results = model.parseResult(model_type, predictions)
```

In this code, we resize the camera frame to be the same size as the image inputs used to trained the model. Next, we perform inference with the model on this resized frame. Finally, use the `awscam.parseResult` to turn the predictions into a dictionary that can be easily parsed. For more information about the output of `parseResult`, see `model.parseResult`.

11. In this step, you add code to send the results back to AWS IoT. This makes it easy to record the results in a database or trigger an action based on the predictions.

In the Lambda code editor, in the function `infinite_infer_run`, under """ Run the DeepLens inference loop frame by frame""", add the following:

```python
# Create an IoT client for sending to messages to the cloud.
client = greengrasssdk.client('iot-data')
iot_topic = '$aws/things/{}/infer'.format(os.environ['AWS_IOT_THING_NAME'])
# Create a local display instance that will dump the image bytes to a FIFO
# file that the image can be rendered locally.
local_display = LocalDisplay('480p')
local_display.start()
```

This code performs two tasks:

- Instantiates an AWS IoT Greengrass SDK (`greengrasssdk`) to make the inference output available to the AWS Cloud. This includes sending process info and processed results to an AWS IoT topic (`iot_topic`). The topic lets you view your AWS DeepLens output as JSON data instead of a video stream.
- Starts a thread (`local_display.start`) to feed parsed video frames for local display (LocalDisplay). The display can be on device (p. 44) or in a web browser (p. 42).

Add the following code after # Send results back to IoT or output to video stream to send the results back frame-by-frame:

```python
# Add the label of the top result to the frame used by local display.
cv2.putText(frame, output_map[top_k[0]['label']], (10, 70),
cv2.FONT_HERSHEY_SIMPLEX, 3, (255, 165, 20), 8)
# Set the next frame in the local display stream.
local_display.set_frame_data(frame)
# Send the top k results to the IoT console via MQTT
cloud_output = {}
for obj in top_k:
    cloud_output[output_map[obj['label']]] = obj['prob']
client.publish(topic=iot_topic, payload=json.dumps(cloud_output))
```

12. Choose Save to save the updated Lambda function. Your function should look like the following:

```python
import json
import awscam
import mo
import cv2
import greengrasssdk
import os
```
from local_display import LocalDisplay

def lambda_handler(event, context):
    """Empty entry point to the Lambda function invoked from the edge."""
    return

def infinite_infer_run():
    """Run the DeepLens inference loop frame by frame""
    # Create an IoT client for sending to messages to the cloud.
    client = greengrasssdk.client('iot-data')
    iot_topic = '$aws/things/{}/infer'.format(os.environ['AWS_IOT_THING_NAME'])

    # Create a local display instance that will dump the image bytes to a FIFO
    # file that the image can be rendered locally.
    local_display = LocalDisplay('480p')
    local_display.start()

    # Load the model here
    # Model details
    input_width = 224
    input_height = 224
    model_name = 'image-classification'
    model_type = 'classification'
    output_map = {0: 'dog', 1: 'cat'}

    # Optimize the model
    error, model_path = mo.optimize(model_name, input_width, input_height)
    # Load the model onto the GPU.
    model = awscam.Model(model_path, {'GPU': 1})

    while True:
        # Get a frame from the video stream
        ret, frame = awscam.getLastFrame()
        # Do inference with the model here
        # Resize frame to the same size as the training set.
        frame_resize = cv2.resize(frame, (input_height, input_width))
        predictions = model.doInference(frame_resize)
        parsed_inference_results = model.parseResult(model_type, predictions)

        k = 2
        # Get top k results with highest probabilities
        top_k = parsed_inference_results[model_type][:0:k]
        print(top_k)
        # Send results back to IoT or output to video stream
        # Add the label of the top result to the frame used by local display.
        cv2.putText(frame, output_map[top_k[0]['label']], (10, 70),
                    cv2.FONT_HERSHEY_SIMPLEX, 3, (255, 165, 20), 8)
        # Set the next frame in the local display stream.
        local_display.set_frame_data(frame)
        # Send the top k results to the IoT console via MQTT
        cloud_output = {}
        for obj in top_k:
            cloud_output[output_map[obj['label']]] = obj['prob']
        client.publish(topic=iot_topic, payload=json.dumps(cloud_output))

        infinite_infer_run()

13. From the Actions dropdown menu list, choose Publish new version. When you publish a function, it becomes available in the AWS DeepLens console and available to add to your custom project.

Create and Deploy a Custom AWS DeepLens Project

Topics
- Create Your Custom Project Using the AWS DeepLens Console (p. 75)
Create Your Custom Project Using the AWS DeepLens Console

The following procedure creates a custom AWS DeepLens project containing a custom-trained model and inference function based on the model. You should have imported your model, created and published a custom inference function before proceeding further.

To create a custom AWS DeepLens project using the AWS DeepLens console

The steps for creating a project encompass two screens. On the first screen you select your project. On the second screen, you specify the project's details.

2. Choose Projects, then choose Create new project.
3. On the Choose project type page, choose Create a new blank project.
4. On the Specify project details page, under Project information, do the following:
   a. In Project name type a name, for example, my-cat-and-dog-detection, to identify your custom project.
   b. Optionally, in Description - Optional provide a description for your custom project.
5. Still on the Specify project details page, under Project content, do the following:
   a. Choose Add model, choose the radio button next to the name of your custom model you've imported into AWS DeepLens, and, then, choose Add model.
   b. Choose Add function, choose the radio button next to the name of your custom inference function you've created and published, and, then, choose Add function.
   If you don't see your function displayed, verify that it's published.
   c. Choose Create to start creating your custom project.
6. On the Projects page, choose the project your just created.
7. Choose Deploy to device and follow the on-screen instructions to deploy the project to your device.

Use SageMaker Neo to Optimize Inference on AWS DeepLens

A trained model might not be optimized to run inference on your device. Before you deploy a trained model to your AWS DeepLens, you can use SageMaker Neo to optimize it to run inference on the AWS DeepLens hardware. The process involves these steps:

1. Compile the model.
2. Import the compiled model into the AWS DeepLens console.
3. Deploy the compiled model to your AWS DeepLens device.
4. Load the compiled model into the Neo runtime of the inference engine.

We recommend that you use Neo-compiled models for improved inference performance with minimal effort on your part.

Topics
• Compile an AWS DeepLens Model (p. 77)
• Import a Compiled Model into the AWS DeepLens Console (p. 77)
• **Load the Compiled Model into the AWS DeepLens Inference Engine (p. 78)**

## Compile an AWS DeepLens Model

To use Neo to compile a model, you can use AWS CLI to create and run a compilation job. First create a job configuration file in JSON to specify the following: The Amazon S3 bucket to load the raw model artifacts from, the training data format, and the machine learning framework, which indicates how the job is to run.

The following example JSON file shows how to specify the job configuration. As an example, the file is named `neo_deeplens.json`.

```json
{
"CompilationJobName": "deeplens_inference",
"RoleArn": "arn:aws:iam::your-account-id:role/service-role/AmazonSageMaker-ExecutionRole-20190429T140091",
"InputConfig": {
"S3Uri": "s3://your-bucket-name/headpose/model/deeplens-tf/train/model.tar.gz",
"DataInputConfig": "{"data": [1,84,84,3]}",
"Framework": "TENSORFLOW"
},
"OutputConfig": {
"S3OutputLocation": "s3://your-bucket-name/headpose/model/deeplens-tf/compile",
"TargetDevice": "deeplens"
},
"StoppingCondition": {
"MaxRuntimeInSeconds": 300
}
}
```

The `InputConfig.S3Uri` property value specifies the S3 path to the trained model artifacts. The `S3OutputLocation` property value specifies the S3 folder to contain the Neo-compiled model artifacts. The input data format specified in the `DataInputConfig` property value must be consistent with the original training data format. For more information about the compilation job configuration property values, see [CreateCompilationJob](#).

To create and run the Neo job, type the following AWS CLI command in a terminal window.

```bash
aws sagemaker create-compilation-job \
--cli-input-json file://neo_deeplens.json \
--region us-west-2
```

In addition to AWS CLI, you can also use the SageMaker console or the SageMaker SDK to create and run the compilation job. To learn more, see use the [SageMaker console](#) and [SageMaker SDK](#) to compile a trained model.

## Import a Compiled Model into the AWS DeepLens Console

This section explains how to import a compiled model. When these steps are complete, you can deploy the model to your AWS DeepLens device and then run inference.

### To import a Neo-compiled model into the AWS DeepLens console

1. Download the compiled model from the S3 folder as specified by the S3OutputLocation path.
2. On your computer, create a folder (compiled-model-folder) to unpack the compiled model into. Note the folder name because you need it later to identify the compiled model.
Building AWS DeepLens Project Tutorials

This section presents end-to-end tutorials to guide your through building, deploying and testing AWS DeepLens projects with deep learning models trained in supported machine learning frameworks.

**Topics**

- **Build and Run the Head Pose Detection Project with TensorFlow-Trained Model (p. 79)**
Build and Run the Head Pose Detection Project with TensorFlow-Trained Model

In this tutorial, we will walk you through an end-to-end process to build and run an AWS DeepLens project to detect head poses. The project is based on the Head pose detection sample project. Specifically, you'll learn:

1. How to train a computer vision model using the TensorFlow framework in SageMaker, including converting the model artifact to the protobuf format for use by AWS DeepLens.
2. How to create an inference Lambda function to infer head poses based on frames captured off the video feed from the AWS DeepLens video camera.
3. How to create an AWS DeepLens project to include the SageMaker-trained deep learning model and the inference Lambda function.
4. How to deploy the project to your AWS DeepLens device to run the project and verify the results.

Topics
- Get the AWS Sample Project on GitHub (p. 79)
- Set Up the Project Data Store in Amazon S3 (p. 81)
- Prepare Input Data for Training In SageMaker (p. 82)
- Train a Head Pose Detection Model in SageMaker (p. 83)
- Create an Inference Lambda Function to Detect Head Poses (p. 88)
- Create and Deploy the Head Pose Detection Project (p. 94)

Get the AWS Sample Project on GitHub

This tutorial is based on the head pose detection sample project (p. 51). The sample project's source code, including the preprocessing script used to prepare for input data from the original Head Pose Image Database, is available on GitHub.
The HeadPose_ResNet50_Tutorial.ipynb file provides a Notebook template as a starting point to learn and explore training our model. The preprocessingDataset_py2.py can be used as-is to prepare input data for training.
You can download and uncompress the zipped GitHub project file to a local drive. Or you can clone the GitHub project. To clone the project, open a terminal window and type the following Git command in a given working directory:

```
git clone https://github.com/aws-samples/headpose-estimator-apache-mxnet
```

By default, the downloaded or cloned project folder is `headpose-estimator-apache-mxnet-master`. We will use this default folder name for the project folder throughout this tutorial.

Having the GitHub project as a template, we're now ready to start building our project by setting up the project's data store in S3 (p. 81).

### Set Up the Project Data Store in Amazon S3

For this project, we will use SageMaker to train the model. To do so, we need to prepare an S3 bucket and four subfolders to store the input needed for the training job and the output produced by the training job.

We will create an Amazon S3 bucket and name it `deeplens-sagemaker-models-<my-name>`. Fill in your name or some ID in the `<my-name>` placeholder to make the bucket name unique. In this bucket, we create a headpose folder to hold data for training the model specific for head pose detection.

We then create the following four subfolders under the headpose folder:

- `deeplens-sagemaker-models-<my-name>/headpose/TFartifacts`: to store training output, i.e., the trained model artifacts.
- `deeplens-sagemaker-models-<my-name>/headpose/customTFcodes`
- `deeplens-sagemaker-models-<my-name>/headpose/datasets`: to store training input, the preprocessed images with known head poses.
- `deeplens-sagemaker-models-<my-name>/headpose/testIMs`

Follow the steps below to create the bucket and folders using the Amazon S3 console:

2. If the Amazon S3 bucket does not exist yet, choose + Create bucket and then type `deeplens-sagemaker-models-<my-name>` in Bucket name, use the default values for other options, and choose Create. Otherwise, double click the existing bucket name to choose the bucket.

3. Choose + Create folder, type the headpose as the folder name, and then choose Save.
4. Choose the headpose folder just created, and then choose + Create folder to create the four subfolders (named TFartifacts, customTFcodes, datasets, testIMs) under headpose, one at a time.
Next, we need to prepared the input data for training in SageMaker (p. 82).

**Prepare Input Data for Training In SageMaker**

The original head pose image database (HeadPoseImageDatabase.tar.gz file) consists of a set of images (.jpeg files) and labels (.txt files) of head poses of 15 persons in a series of tilt and pan positions. They must be transformed to a single .pkl file as the input to an SageMaker training job.

To prepare the training data, you can use the preprocessing script (preprocessingDataset_py2.py) provided in the Head Pose Sample Project on Github (p. 79). You can run this script on your computer locally or on the AWS Cloud through a Python Notebook instance. In this section, you'll learn how to prepare the training data locally. You'll learn how to do it in a Notebook instance in the section called “Train a Head Pose Detection Model in SageMaker” (p. 83).

1. Open a terminal and change directory to the directory where to you downloaded the head pose sample project (p. 79).
2. Run the following Python (version 2.7) command

   ```
   python preprocessingDataset_py2.py --num-data-aug 15 --aspect-ratio 1
   ```
If you get an error stating that the cv2 module is not found, run the following command to install the missing module:

```bash
python -m pip install opencv-python
```

Then, rerun the preprocessing script.

The process takes 15-20 hours to complete. The preprocessing script outputs the results as the HeadPoseData_trn_test_x15_py2.pkl file in the current working directory.

3. Upload the preprocessed training data (HeadPoseData_trn_test_x15_py2.pkl) file into the deeplens-sagemaker-models-<my-name>/headpose/datasets folder in Amazon S3. You can do this using the Amazon S3 console or, as shown as follows, using the following AWS CLI command:

```bash
aws s3 cp HeadPoseData_trn_test_x15_py2.pkl s3://deeplens-sagemaker-models-<my-name>/headpose/datasets
```

**Note**
Instead of running locally, you can prepare the input data on the AWS Cloud by a code cell in a SageMaker notebook instance, where cv2 and Python 2.7 (python2) are readily available, and run the commands in Step 2 and Step 3, respectively, as follows:

```bash
!python2 preprocessingDataset_py2.py --num-data-aug 15 --aspect-ratio 1
```

and

```bash
!aws s3 cp HeadPoseData_trn_test_x15_py2.pkl s3://deeplens-sagemaker-models-<my-name>/headpose/datasets
```

You notebook instance needs to run on a sufficiently powerful EC2 instance of, e.g., the ml.p2.xlarge type.

Now that we have the input data prepared and stored in S3, we’re ready to train the model (p. 83).

**Train a Head Pose Detection Model in SageMaker**

To train our model in SageMaker, follow the steps below to create a Notebook using the SageMaker console:

**Create an SageMaker Notebook**

2. From the main navigation pane, choose Notebook instances.
3. Under Notebook instance settings on the Create notebook instance page, do the following:
   a. Under Notebook instance name, type TFHeadpose.
   b. Leave the default values for all other options.
   c. Choose Create notebook instance.
4. Next to the TFHeadpose notebook instance, choose Open, after the notebook instance status becomes inService.
5. On the upper-right corner, choose Upload to start importing a notebook instance and other needed files.
6. In the file picker, navigate to the `HeadPost_SageMaker_PythonSDK` folder in the previously cloned or downloaded `headpose-estimator-apache-mxnet-master` project folder. Then, select the following files:

   - `resnet_headpose.py`: This is a script that defines the workflow for training with the deep learning network architecture prescribed in the accompanying `resnet_model_headpose.py` file applied to a specified input data.
   - `resnet_model_headpose.py`: This is a Python script that prescribes the deep learning network architecture used to train our model for head pose detection.
   - `tensorflow_resnet_headpost_for_deeplens.ipynb`: This is a Notebook instance to run an SageMaker job to manage training following the script of `resnet_headpose.py`, including data preparation and transformation.

Then, choose Open.

If you intend to run the preprocessing script on the AWS Cloud, navigate to the `headpose-estimator-apache-mxnet-master` folder, select the `preprocessingDataset_py2.py`, and choose Open.

7. On the Files tab in the TFHeadpose notebook, choose Upload for each of the newly selected files to finish importing the files into the notebook. You're now ready to run an SageMaker job to train your model.

8. Choose `tensorflow_resnet_headpose_for_deeplens.ipynb` to open the notebook instance in a separate browser tab. The notebook instance lets you step through the tasks necessary to run an SageMaker job to train your model and to transform the model artifacts to a format supported by AWS DeepLens.

9. Run an SageMaker job to train your model in the notebook instance. The implementation is presented in separate code cells that can be run sequentially.

   a. Under Set up the environment, the code cell contains the Python code to configure the data store for the input and output of the SageMaker model training job.

   ```python
   import os
   import sagemaker
   from sagemaker import get_execution_role

   s3_bucket = 'deeplens-sagemaker-models-<my-name>'
   headpose_folder = 'headpose'

   #Bucket location to save your custom code in tar.gz format.
   custom_code_folder = 'customTFcodes'
   custom_code_upload_location = 's3://{}/{}/{}'.format(s3_bucket, headpose_folder, custom_code_folder)

   #Bucket location where results of model training are saved.
   model_artifacts_folder = 'TFartifacts'
   model_artifacts_location = 's3://{}/{}/{}'.format(s3_bucket, headpose_folder, model_artifacts_folder)

   #IAM execution role that gives SageMaker access to resources in your AWS account.
   #We can use the SageMaker Python SDK to get the role from our notebook environment.
   role = get_execution_role()
   ```

To use the S3 bucket and folders (p. 81) as the data store, assign your S3 bucket name (e.g., `deeplens-sagemaker-models-<my-name>`) to the `s3_bucket` variable. Make sure that the specified folder names all match what you have in the Amazon S3 bucket.
To execute this code block, choose Run from the menu bar of the notebook instance.

b. Under Create a training job using the sagemaker.tensorflow.TensorFlow estimator, the code cell contains the code snippet that performs the following tasks:

1. Instantiate a `sagemaker.tensorflow.TensorFlow` estimator class (`estimator`), with a specified training script and process configuration.

2. Start training the model (`estimator.fit(...)` with the estimator, with the training data in a specified data store.

The code snippet is shown as follows:

```python
from sagemaker.tensorflow import TensorFlow

source_dir = os.path.join(os.getcwd())

# AWS DeepLens currently supports TensorFlow version 1.4 (as of August 24th 2018).
# Head-pose dataset "HeadPoseData_trn_test_x15_py2.pkl" is in the following S3 folder.
dataset_location = 's3://{}/datasets'.format(s3_bucket, headpose_folder)

estimator = TensorFlow(entry_point='resnet_headpose.py',
                        framework_version = 1.4,
                        source_dir=source_dir,
                        role=role,
                        training_steps=25000, evaluation_steps=700,
                        train_instance_count=1,
                        base_job_name='deeplens-TF-headpose',
                        output_path=model_artifacts_location,
                        code_location=custom_code_upload_location,
                        train_instance_type='ml.p2.xlarge',
                        train_max_run = 432000,
                        train_volume_size=100)
```

85
To create the estimator object, you assign to entry_point the name of the Python file containing the custom TensorFlow model training script. For this tutorial, this custom code file is `resnet_headpose.py` that was uploaded to the same directory where the notebook instance is located. For framework_version, specify a TensorFlow version supported by AWS DeepLens.

With the `train_instance_type` of `ml.p2.xlarge`, it takes about 6.7 billable compute hours to complete the training job (estimator.fit(...)). You can experiment with other `train_instance_type` options to speed up the process or to optimize the cost.

The successfully trained model artifact (model.tar.gz) is output to your S3 bucket:

```
s3://deeplens-sagemaker-models-<my-name>/headpose/TFartifacts/<training-job-name>/output/model.tar.gz
```

where `<training-job-name>` is of the `<base_job_name>-<timestamp>`. Using the training code above, an example of the `<training-job-name>` would be `deeplens-TF-headpose-2018-08-16-20-10-09-991`. You must transform this model artifact into a frozen protobuff format that is supported by AWS DeepLens.

c. To transform the trained model artifact (model.tar.gz) into a frozen protobuff file (frozen.model.pb), do the following:

i. Run the following code to use the AWS SDK for Python (boto3) in a code cell in the notebook to download the trained model artifact from your S3 bucket to your notebook:

```python
import boto3
s3 = boto3.resource('s3')
#key = '{}/{}/output/model.tar.gz'.format(headpose_folder, model_artifacts_folder, estimator.latest_training_job.name)
key = '{}/{}/output/model.tar.gz'.format(headpose_folder, model_artifacts_folder, 'deeplens-TF-headpose-2018-08-16-20-10-09-991')
print(key)
s3.Bucket(s3_bucket).download_file(key, 'model.tar.gz')
```

You can verify the downloaded files by running the following shell command in a code cell of the notebook and then examine the output.

```
!ls
```

ii. To uncompress the trained model artifact (model.tar.gz), run the following shell command in a code cell:

```
!tar -xvf model.tar.gz
```

This command will produce the following output:

```
export/
export/Servo/
export/Servo/1534474516/
export/Servo/1534474516/variables/
export/Servo/1534474516/variables/variables.data-00000-of-00001
export/Servo/1534474516/variables/variables.index
```
export/Servo/1534474516/saved_model.pb

The path to a model directory is of the export/*/ pattern. You must specify the model directory path to make a frozen protobuff file from the model artifact. You'll see how to get this directory path in the next step.

iii. To get the model directory and cache it in memory, run the following Python code in a code cell of the notebook instance:

```python
import glob
model_dir = glob.glob('export/*/*')
# The model directory looks like 'export/Servo/{Assigned by Amazon SageMaker}'}
print(model_dir)
```

The output is `['export/Servo/1534474516']`.

You can proceed to freezing the graph and save it in the frozen protobuff format.

iv. To freeze the TensorFlow graph and save it in the frozen protobuff format, run the following Python code snippet in a code cell of the notebook instance. The code snippet does the following:

1. Calls `tf.graph_util.convert_variables_to_constants` to freeze the graph,
2. Calls `tf.graph_util.remove_training_nodes` to remove all unnecessary nodes.
3. Calls `optimize_for_inference` to generate the inference graph_def.
4. Serializes and saves the file as a protobuff.

```python
import tensorflow as tf
from tensorflow.python.tools import optimize_for_inference_lib
def freeze_graph(model_dir, input_node_names, output_node_names):
    # Extract the sub graph defined by the output nodes and convert all its variables into constant
    # Args:
    # model_dir: the root folder containing the checkpoint state file,
    # input_node_names: a comma-separated string, containing the names of all input nodes
    # output_node_names: a comma-separated string, containing the names of all output nodes,
    
    # We start a session using a temporary fresh Graph
    with tf.Session(graph=tf.Graph()) as sess:
        # We import the meta graph in the current default Graph
        tf.saved_model.loader.load(sess, [tf.saved_model.tag_constants.SERVING], model_dir)

        # We use a built-in TF helper to export variables to constants
        input_graph_def = tf.graph_util.convert_variables_to_constants(sess, # The session is used to retrieve the weights
            tf.get_default_graph().as_graph_def(), # The graph_def is used to retrieve the nodes
            output_node_names.split(','), # The output node names are used to select the usefull nodes
        )

        # We generate the inference graph_def
```
input_node_names=['Const_1']  # an array of the input node(s)
output_graph_def =
    optimize_for_inference_lib.optimize_for_inference(tf.graph_util.remove_training_nodes(input_graph_def),
    input_node_names.split(','),  # an array of input nodes
    output_node_names.split(','),  # an array of output nodes
    tf.float32.as_datatype_enum)

    # Finally we serialize and dump the output graph_def to the filesystem
    with tf.gfile.GFile('frozen_model.pb', "wb") as f:
            f.write(output_graph_def.SerializeToString())

    freeze_graph(model_dir[0], 'Const_1', 'softmax_tensor')

As the result, the model artifact is transformed into the frozen protobuff format (frozen_model.pb) and saved to the notebook instance's home directory (model_dir[0]).

In the code above, you must specify the input and output nodes, namely, 'Const_1' and 'softmax_tensor'. For more details, see the resnet_model_headpose.py.

When creating an AWS DeepLens project later, you'll need to add this frozen graph to the project. For this you must upload the protobuff file to an Amazon S3 folder. For this tutorial, you can use your SageMaker training job's output folder (s3://deeplens-sagemaker-models-{my-name}/headpose/TFartifacts/{sagemaker-job-name}/output) in S3. However, the model is considered an externally trained model in AWS DeepLens.

d. To upload the frozen graph to your SageMaker training job's output folder, run the following Python code snippet in a code cell of the running notebook instance:

```python
data = open('frozen_model.pb', "rb")
#key = '{}/{}{}'.format(headpose_folder, model_artifacts_folder,estimator.latest_training_job.name)
key = '{}/{}{}'.format(headpose_folder, model_artifacts_folder, 'deeplens-TF-headpose-2018-08-16-20-10-09-991')
s3.Bucket(s3_bucket).put_object(Key=key, Body=data)
```

Once uploaded, the model is ready to be imported into your AWS DeepLens project. Before creating the project, we must create a Lambda function that performs inference based on this trained model (p. 88).

Create an Inference Lambda Function to Detect Head Poses

Before creating an AWS DeepLens project for deployment to your AWS DeepLens device for head pose detection, you must create and publish a Lambda function to make inference based on the trained model.

To create and publish the inference Lambda function, follow the instruction given in the section called "Create and Publish an Inference Lambda Function" (p. 71), but replace the code in the greengrassHelloWorld.py file with one similar to the following that is used in the Head Pose Detection Sample project (p. 51).

```python
""" This is a lambda function that demonstrates how one can use a deep learning network (ResNet) to detect the person's head pose. We use a shaded rectangle to indicate the region that the person's head is pointed towards. We also display a red ball that moves with the person's head.
"""
```
from threading import Thread, Event
import os
import json
import numpy as np
import cv2
import greengrasssdk
import awscam
import mo

class LocalDisplay(Thread):
    """ Class for facilitating the local display of inference results (as images). The class is designed to run on its own thread. In particular the class dumps the inference results into a FIFO located in the tmp directory (which lambda has access to). The results can be rendered using mplayer by typing:
    mplayer -demuxer lavf -lavfdopts format=mjpeg:probesize=32 /tmp/results.mjpeg
"""
    def __init__(self, resolution):
        """ resolution - Desired resolution of the project stream"
        # Initialize the base class, so that the object can run on its own thread.
        super(LocalDisplay, self).__init__()
        # List of valid resolutions
        RESOLUTION = {'1080p': (1920, 1080), '720p': (1280, 720), '480p': (858, 480)}
        if resolution not in RESOLUTION:
            raise Exception("Invalid resolution")
        self.resolution = RESOLUTION[resolution]
        # Initialize the default image to be a white canvas. Clients will update the image when ready.
        self.frame = cv2.imencode('.jpg', 255*np.ones([640, 480, 3]))[1]
        self.stop_request = Event()

    def run(self):
        """ Overridden method that continually dumps images to the desired FIFO file."
        # Path to the FIFO file. The lambda only has permissions to the tmp directory. Pointing to a FIFO file in another directory will cause the lambda to crash.
        result_path = '/tmp/results.mjpeg'
        # Create the FIFO file if it doesn't exist.
        if not os.path.exists(result_path):
            os.mkfifo(result_path)
        # This call will block until a consumer is available with open(result_path, 'w') as fifo_file:
        with open(result_path, 'w') as fifo_file:
            while not self.stop_request.isSet():
                try:
                    # Write the data to the FIFO file. This call will block meaning the code will come to a halt here until a consumer is available.
                    fifo_file.write(self.frame.tobytes())
                except IOError:
                    continue

    def set_frame_data(self, frame):
        """ Method updates the image data. This currently encodes the numpy array to jpg but can be modified to support other encodings."
        frame = cv2.imencode('.jpg', cv2.resize(frame, self.resolution))
        if not frame:
            raise Exception('Failed to set frame data')
        self.frame = jpg
def join(self):
    self.stop_request.set()

class HeadDetection():
    """ Custom class that helps us post process the data. In particular it draws
    a ball that moves across the screen depending on the head pose.
    It also draws a rectangle indicating the region that the person's head is pointing
    to. We divide the frame into 9 distinct regions.
    """
    def __init__(self, circ_cent_x, circ_cent_y):
        """ circ_cent_x - The x coordinate for the center of the frame
        circ_cent_y - The y coordinate for the center of the frame
        """
        self.result_thread = LocalDisplay('480p')
        self.result_thread.start()
        self.circ_cent_x = circ_cent_x
        self.circ_cent_y = circ_cent_y
        # Compute the maximum x and y coordinates.
        self.x_max = 2 * circ_cent_x
        self.y_max = 2 * circ_cent_y
        # Number of quadrants to split the image into.
        # This is model dependent.
        self.quadrants = 9

    def update_coords(self, frame, change_x, change_y, label):
        """ Helper method that draws a rectangle in the region the person is looking at.
        It also draws a red ball that changes its speed based on how long a person
        has been looking at a particular direction.
        frame - The frame where the ball and rectangle should be drawn
        change_x - The amount to increment the x axis after drawing the red ball.
        change_y - The amount to increment the y axis after drawing the red ball.
        label - Label corresponding to the region that the person's head is looking at.
        """
        # Set coordinates of the rectangle that will be drawn in the region that the
        # person is looking at.
        rect_margin = 10
        rect_width = frame.shape[1] // 3 - rect_margin * 2
        rect_height = frame.shape[0] // 3 - rect_margin * 2
        # Set the draw options.
        overlay = frame.copy()
        font_color = (20, 165, 255)
        line_type = 8
        font_type = cv2.FONT_HERSHEY_DUPLEX
        # Draw the rectangle with some text to indicate the region.
        if label == 0:
            cv2.putText(frame, "Down Right", (1024, 440 - 15), font_type, 3, font_color,
                        line_type)
            cv2.rectangle(overlay,
                          (frame.shape[1] // 3 * 2 + rect_margin,
                           frame.shape[0] // 3 * 2 + rect_margin),
                          (frame.shape[1] // 3 * 2 + rect_width,
                           frame.shape[0] // 3 * 2 + rect_height),
                          (0, 255, 0), -1)
        elif label == 1:
            cv2.putText(frame, "Right", (1024, 440 - 15), font_type, 3, font_color,
                        line_type)
            cv2.rectangle(overlay,
                          (frame.shape[1] // 3 * 2 + rect_margin,
                           frame.shape[0] // 3 * 1 + rect_margin),
                          (frame.shape[1] // 3 * 2 + rect_width,
                           frame.shape[0] // 3 * 1 + rect_height),
                          (0, 255, 0), -1)
        elif label == 2:
            cv2.putText(frame, "Up Right", (1024, 440 - 15), font_type, 3, font_color,
                        line_type)
            cv2.rectangle(overlay,
elif label == 3:
    cv2.putText(frame, "Down", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay,
                 (frame.shape[1] // 3 * 1 + rect_margin, rect_margin),
                 (frame.shape[1] // 3 * 1 + rect_width, rect_height),
                 (0, 255, 0), -1)
elif label == 4:
    cv2.putText(frame, "Middle", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay,
                 (frame.shape[1] // 3 * 1 + rect_margin, rect_margin),
                 (frame.shape[1] // 3 * 1 + rect_width, rect_height),
                 (0, 255, 0), -1)
elif label == 5:
    cv2.putText(frame, "Up", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay,
                 (frame.shape[1] // 3 * 1 + rect_margin, rect_margin),
                 (frame.shape[1] // 3 * 1 + rect_width, rect_height),
                 (0, 255, 0), -1)
elif label == 6:
    cv2.putText(frame, "Down Left", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay,
                 (rect_margin, frame.shape[0] // 3 * 2 + rect_margin),
                 (rect_width, frame.shape[0] // 3 * 2 + rect_height),
                 (0, 255, 0), -1)
elif label == 7:
    cv2.putText(frame, "Left", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay,
                 (rect_margin, frame.shape[0] // 3 * 1 + rect_margin),
                 (rect_width, frame.shape[0] // 3 * 1 + rect_height),
                 (0, 255, 0), -1)
else:
    cv2.putText(frame, "Up Left", (1024, 440 - 15), font_type, 3, font_color, line_type)
    cv2.rectangle(overlay, (rect_margin, rect_margin),
                 (rect_width, rect_height), (0, 255, 0), -1)
# Set the opacity
alpha = 0.2
cv2.addWeighted(overlay, alpha, frame, 1 - alpha, 0, frame)
# Draw the red ball at the previous x-y position.
cv2.circle(frame, (self.circ_cent_x, self.circ_cent_y), 50, (0, 0, 255), -1)
# Update the balls x-y coordinates.
selself.circ_cent_x += int(change_x)
selself.circ_cent_y += int(change_y)
# Make sure the ball stays inside the image.
if self.circ_cent_x > self.x_max:
    self.circ_cent_x = self.x_max
if self.circ_cent_x < 0:
    self.circ_cent_x = 0
if self.circ_cent_y > self.y_max:
    self.circ_cent_y = self.y_max
if self.circ_cent_y < 0:
    self.circ_cent_y = 0
# Send the post processed frame to the FIFO file for display
self.result_thread.set_frame_data(frame)
def adjust_x_vel(self, velocity, pct_of_center):
    """ Helper for computing the next x coordinate.
    velocity - x direction velocity.
    pct_of_center - The percentage around the center of the image that
    we should consider a dead zone.
    """
    x_vel = 0
    if self.circ_cent_x < (1.0 - pct_of_center) * self.x_max/2:
        x_vel = velocity
    if self.circ_cent_x > (1.0 - pct_of_center) * self.x_max/2:
        x_vel = -1 * velocity
    return x_vel

def adjust_y_vel(self, velocity, pct_of_center):
    """ Helper for computing the next y coordinate.
    velocity - y direction velocity.
    pct_of_center - The percentage around the center of the image that
    we should consider a dead zone.
    """
    y_vel = 0
    if self.circ_cent_y < (1.0 - pct_of_center) * self.y_max/2:
        y_vel = velocity
    if self.circ_cent_y > (1.0 - pct_of_center) * self.y_max/2:
        y_vel = -1 * velocity
    return y_vel

def send_data(self, frame, parsed_results):
    """ Method that handles all post processing and sending the results to a FIFO file.
    frame - The frame that will be post processed.
    parsed_results - A dictionary containing the inference results.
    """
    label = parsed_results[0]['label']
    # Use the probability to determine the velocity, scale it by 100 so that the ball
    # moves across the screen at reasonable rate.
    velocity = parsed_results[0]['prob'] * 100
    pct_of_center = 0.05
    if label == 0:
        self.update_coords(frame, velocity, velocity, label)
    elif label == 1:
        self.update_coords(frame, velocity, self.adjust_y_vel(velocity, pct_of_center), label)
    elif label == 2:
        self.update_coords(frame, self.adjust_x_vel(velocity, pct_of_center), velocity, label)
    elif label == 3:
        self.update_coords(frame, self.adjust_x_vel(velocity, pct_of_center), self.adjust_y_vel(velocity, pct_of_center), label)
    elif label == 4:
        self.update_coords(frame, self.adjust_x_vel(velocity, pct_of_center), -1*velocity, label)
    elif label == 5:
        self.update_coords(frame, -1*velocity, velocity, label)
    elif label == 6:
        self.update_coords(frame, -1*velocity, self.adjust_y_vel(velocity, pct_of_center), label)
    elif label == 7:
        self.update_coords(frame, -1*velocity, -1*velocity, label)
    elif label == 8:
        self.update_coords(frame, -1*velocity, -1*velocity, label)

def get_results(self, parsed_results, output_map):
    """ Method converts the user entered number of top inference
    labels and associated probabilities to json format.
parsed_results - A dictionary containing the inference results.
output_map - A dictionary that maps the numerical labels returned
the inference engine to human readable labels.

if self.quadrants <= 0 or self.quadrants > len(parsed_results):
    return json.dumps({'Error': 'Invalid'})

top_result = parsed_results[0:self.quadrants]
cloud_output = {}
for obj in top_result:
    cloud_output[output_map[obj['label']]] = obj['prob']
return json.dumps(cloud_output)

def head_detection():
    """ This method serves as the main entry point of our lambda. """
    # Creating a client to send messages via IoT MQTT to the cloud
    client = greengrasssdk.client('iot-data')
    # This is the topic where we will publish our messages to
    iot_topic = '${AWS_IOT_THING_NAME}/infer'
    try:
        # define model prefix and the amount to down sample the image by.
        input_height = 84
        input_width = 84
        model_name='frozen_model'
        # Send message to IoT via MQTT
        client.publish(topic=iot_topic, payload="Optimizing model")
        ret, model_path = mo.optimize(model_name, input_width, input_height, platform='tf')
        # Send message to IoT via MQTT
        client.publish(topic=iot_topic, payload="Model optimization complete")
        if ret is not 0:
            raise Exception("Model optimization failed, error code: {}".format(ret))
        # Send message to IoT via MQTT
        client.publish(topic=iot_topic, payload="Loading model")
        # Load the model into cl-dnn
        model = awscam.Model(model_path, {'GPU': 1})
        # Send message to IoT via MQTT
        client.publish(topic=iot_topic, payload="Model loaded")
        # We need to sample a frame so that we can determine where the center of
        # the image is located. We assume that
        # resolution is constant during the lifetime of the Lambda.
        ret, sample_frame = awscam.getLastFrame()
        if not ret:
            raise Exception("Failed to get frame from the stream")
        # Construct the custom helper object. This object just lets us handle
        postprocessing
        head_pose_detection = HeadDetection(sample_frame.shape[1]/2,
                                              sample_frame.shape[0]/2)
        # Dictionary that will allow us to convert the inference labels
        # into a human a readable format.
        output_map = {{0:'Bottom Right', 1:'Middle Right', 2:'Top Right', 3:'Bottom
        Middle',
                      4:'Middle Middle', 5:'Top Middle', 6:'Bottom Left', 7:'Middle Left',
                      8:'Top Left'}}
        # This model is a ResNet classifier, so our output will be classification.
        model_type = "classification"
        # Define a rectangular region where we expect the persons head to be.
        crop_upper_left_y = 440
        crop_height = 640
        crop_upper_left_x = 1024
        crop_width = 640
        while True:
            # Grab the latest frame off the mjjpeg stream.
            ret, frame = awscam.getLastFrame()
            if not ret:
Build and Run the Head Pose Detection Project

```python
raise Exception("Failed to get frame from the stream")
# Mirror Image
frame = cv2.flip(frame, 1)
# Draw the rectangle around the area that we expect the persons head to be.
cv2.rectangle(frame, (crop_upper_left_x, crop_upper_left_y),
              (crop_upper_left_x + crop_width, crop_upper_left_y + crop_height),
              (255, 40, 0), 4)
# Crop the the frame so that we can do inference on the area of the frame where
# expect the persons head to be.
frame_crop = frame[crop_upper_left_y:crop_upper_left_y + crop_height, crop_upper_left_x:crop_upper_left_x + crop_width]
# Down sample the image.
frame_resize = cv2.resize(frame_crop, (input_width, input_height))
# Renormalize the image so that the color magnitudes are between 0 and 1
frame_resize = frame_resize.astype(np.float32)/255.0
# Run the down sampled image through the inference engine.
infer_output = model.doInference(frame_resize)
# Parse the results so that we get back a more manageable data structure.
parsed_results = model.parseResult(model_type, infer_output)[model_type]
# Post process the image and send it to the FIFO file
head_pose_detection.send_data(frame, parsed_results)
# Send the results to MQTT in JSON format.
client.publish(topic=iot_topic, payload=head_pose_detection.get_results(parsed_results, output_map))
except Exception as ex:
    msg = "Lambda has failure, error msg {}": "{}.format(ex)
    client.publish(topic=iot_topic, payload=msg)
# Entry point of the lambda function.
head_detection()
```

The `LocalDisplay` class defined in the Lambda function above serializes processed images, in a dedicated thread, to a specified FIFO file that serves as the source to replay the inference results as the project stream.

The `HeadDetection` class handles post-process of parsed data, including calling out a detected head position and pose in the project stream's local display.

The `head_detection` function coordinates the whole process to infer head poses of capture frames from AWS DeepLens video feeds, including loading the model artifact deployed to your AWS DeepLens device. To load the model, you must specify the path to the model artifact. To get this path you can call the `mo.optimize` method and specify "frozen_model" as the `model_name` input value. This model name corresponds to the file name without the .pb extension of the model artifact uploaded to Amazon S3.

Having trained your model and uploaded it to S3 and created the Lambda function in your account, you're now ready to create and deploy the head pose detection project (p. 94).

Create and Deploy the Head Pose Detection Project

Before creating the AWS DeepLens project, you must import the model into AWS DeepLens. Because the original SageMaker-trained model artifact is converted to a protobuff file, you must treat the transformed model artifact as externally trained.

To import the customized SageMaker-trained model for head pose detection

1. Go to the AWS DeepLens console.
2. Choose **Models** from the main navigation pane.
3. Choose **Import model**.
4. On the **Import model to AWS DeepLens** page, do the following:
   a. Under **Import source**, choose **Externally trained model**.
   b. Under **Model settings**, do the following:
      i. For **Model artifact path**, type the model's S3 URL, e.g., `s3://deeplens-sagemaker-models-<my-name>/headpose/TFartifacts/<sagemaker-job-name>/output/frozen_model.pb`.
      ii. For **Model name**, type a name for your model, e.g., `my-headpose-detection-model`.
      iii. For **Model framework**, choose ```TensorFlow```.
      iv. For **Description - Optional**, type a description about the model, if choose to do so.

After importing the model, you can now create an AWS DeepLens project to add the imported model and the published inference Lambda function.

**To create a custom AWS DeepLens project for head pose detection**

1. In the AWS DeepLens console, choose **Projects** from the main navigation pane.
2. In the **Projects** page, choose **Create new project**.
3. On the **Choose project type** page, choose **Create a new blank project**. Then, choose **Next**.
4. On the **Specify project details** page, do the following:
   - Under **Project information**, type a name for your project in the **Project name** input field and, optionally, give a project description in the **Description - Optional** input field.
5. Under **Project content**, do the following:
   a. Choose **Add model**. Then, select the radio button next to your head pose detection model imported earlier and choose **Add model**.
   b. Choose **Add function**. Then, select the radio button next to the published Lambda function for head pose detection and choose **Add function**.

   The function must be published in AWS Lambda and named with the `deeplens-` prefix to make it visible here. If you've published multiple versions of the function, make sure to choose the function of the correction version.
6. Choose **Create**.

With the project created, you're ready to deploy it to your registered AWS DeepLens device. Make sure to remove any active project from the device before proceeding further.

1. In the **Projects** page of the DAWS DeepLensL console, choose the newly created project for head pose detection.
2. In the selected project details page, choose **Deploy to device**.
3. On the **Target device** page, select the radio button next to your registered device and then choose **Review**.
4. On the **Review and deploy** page, choose **Deploy** after verifying the project details.
5. On the device details page, examine the deployment status by inspecting **Device status** and **Registration status**. If they're **Online** and **Registered**, respectively, the deployment succeeded. Otherwise, verify that the imported model and the published Lambda function are valid.
6. After the project is successfully deployed, you can view the project output in one of the following ways:
a. View the JSON-formatted output published by the inference Lambda function in the AWS IoT Core console.

b. View streaming video in a supported web browser. For instructions, the section called "View Video Stream from AWS DeepLens Device in Browser." (p. 42).

This completes this tutorial to build and deploy your head pose detection project.
Managing Your AWS DeepLens Device

The following topics explain how to manage your AWS DeepLens device and access device resource from a AWS IoT Greengrass Lambda function:

Topics

- Securely Boot Your AWS DeepLens Device (p. 97)
- Update Your AWS DeepLens Device (p. 97)
- Deregistering Your AWS DeepLens Device (p. 98)
- Deleting AWS DeepLens Resources (p. 99)
- Restoring your AWS DeepLens device to Factory Settings (p. 100)

Securely Boot Your AWS DeepLens Device

To protect the AWS DeepLens device from malicious attacks, it is configured to boot securely. The secure boot settings prevent the device from loading unauthorized operating systems, including versions that are under mainstream support. If an attacker bypasses the secure boot settings and loads other operating systems or other versions, the device could become unstable and the warranty will be void.

Update Your AWS DeepLens Device

When you set up your device, you had the option to enable automatic updates (see Set Up Your AWS DeepLens Device (p. 27)). If you enabled automatic updates, you need only to reboot the device to get the software updated on your device. If you didn't enable automatic updates, you need to manually update your device periodically.

Note

If your updates gets stuck in an endless loop, try to check and turn on the Unsupported updates option under Install updates from: on the Updates tab in Software & Updates, an Ubuntu system utility on the device.

To manually update your AWS DeepLens on the device

1. Plug in your AWS DeepLens and turn it on.
2. Use a micro HDMI cable to connect your AWS DeepLens to a monitor.
3. Connect a USB mouse and keyboard to your AWS DeepLens.
4. When the login screen appears, sign in to the device using the SSH password you set when you registered it.
5. Start your terminal and run each of the following commands:

```
sudo apt-get update
sudo apt-get install awscam
```
To manually update your AWS DeepLens using an SSH terminal

1. Go to the AWS DeepLens console, and do the following:
   a. Choose Devices from the main navigation pane.
   b. From the device list, choose your AWS DeepLens device to open the device information page.
   c. From the Device details section, copy a local IP address of the selected AWS DeepLens device.

2. Start a terminal and type the following SSH command, using the above example's IP address (192.168.1.36):

   ```
   ssh aws_cam@192.168.1.36
   ```

3. Run each of the following commands:

   ```
   sudo apt-get update
   sudo apt-get install awscam
   sudo reboot
   ```

Deregistering Your AWS DeepLens Device

Deregistering your AWS DeepLens disassociates your AWS account and credentials from the device. Before you deregister your device, delete the photos or videos that are stored on it.

To deregister your AWS DeepLens

2. From the primary navigation pane, choose Devices, then choose the device that you want to deregister.
3. Next to the Current project on the selected device page, choose Remove current project from device.

   **Important**
   Delete the photos or videos that are stored on the device, using SSH and the SSH password that you set when you registered the device to log on to the device. Navigate to the folder where the photos or videos are stored and delete them.

4. When prompted, choose Yes to confirm.
5. Next to Device Settings, choose Deregister.
6. When prompted, choose Deregister to confirm.
Your AWS DeepLens is now deregistered. To use it again, repeat each of these steps:

- Register Your AWS DeepLens Device (p. 9)
- Connect to Your AWS DeepLens Device’s Wi-Fi Network (p. 23)
- Set Up Your AWS DeepLens Device (p. 27)
- Verify Your AWS DeepLens Device Registration Status (p. 31)

Deleting AWS DeepLens Resources

When you build your computer vision application and deploy it to your AWS DeepLens device, you store AWS DeepLens resources—such as a device profile, a deployed project, and a model—in the AWS Cloud. When you are done with your AWS DeepLens project, you can use the AWS console to delete the model, project, and AWS DeepLens logs from CloudWatch Logs. To delete a registered device profile, see Deregistering Your AWS DeepLens Device (p. 98).

Topics

- Delete AWS DeepLens Resources Using the AWS Console (p. 99)

Delete AWS DeepLens Resources Using the AWS Console

Topics

- Delete an AWS DeepLens Project (p. 99)
- Delete an AWS DeepLens Model (p. 99)
- Delete an AWS DeepLens Device Profile (p. 100)
- Delete AWS DeepLens Logs from CloudWatch Logs (p. 100)

Delete an AWS DeepLens Project

2. In the navigation pane, choose Projects.
3. On the Projects page, choose the button next to the project that you want to delete.
4. In the Actions list, choose Delete.
5. In the Delete project-name dialog box, choose Delete to confirm that you want to delete the project.

Delete an AWS DeepLens Model

2. In the navigation pane, choose Models.
3. On the Models page, choose the button next to the model that you want to delete.
4. In the Action list, choose Delete.
5. In the Delete model-name dialog box, choose Delete to confirm that you want to delete the model.
Delete an AWS DeepLens Device Profile

To deleting an unused device profile, you deregister the device. For more information, see Deregistering Your AWS DeepLens Device (p. 98).

Delete AWS DeepLens Logs from CloudWatch Logs

If you exposed personally identifiable information in the AWS IoT Greengrass user logs that were created in Amazon CloudWatch Logs when you ran your AWS DeepLens project, use the CloudWatch Logs console to delete them.

1. Sign in to the AWS Management Console and open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose Logs.
3. On the Log Groups page, choose the button next to the AWS IoT Greengrass user log that you want to delete. The log begins with /aws/greengrass/Lambda/....
4. In the Actions list, choose Delete log group.
5. In the Delete log group dialog box, choose Yes, Delete to confirm that you want to delete the logs.

Note
When the Lambda function for your project runs again, the deleted log group will be recreated.

Restoring your AWS DeepLens device to Factory Settings

After using your AWS DeepLens, you may want to reset the device to its factory settings. Resetting the AWS DeepLens requires multiple steps. First, you must partition a USB drive into two parts and make the first partition bootable. Next, you also need to download the required files for the factory restore. These files are greater than 10 GB combined. Finally, The second procedure explains how to use the partitioned flash drive and its contents to restore your AWS DeepLens to its factory settings.

• Partitioning a USB drive into two parts. (p. 100)
• Using a partitioned USB drive to restore your AWS DeepLens device (p. 106)

Preparing to perform factory reset on your AWS DeepLens device

Resetting your AWS DeepLens completely removes any data on the device and returns it to its factory settings. This process requires additional hardware. This topic explains what you need to get started and walks you through the process.

Prerequisites

Before starting, make sure you have the following items ready:

• 1 USB drive, 16 GB or larger
• A DeepLens (v1.0) or a AWS DeepLens 2019 Edition(v1.1) device.

To learn more about AWS DeepLens versions, see the section called “Device Versions” (p. 1).
Preparing to perform factory reset on your AWS DeepLens device

- A computer to facilitate preparation:
  - You can set up your AWS DeepLens camera as a Linux computer using a pointer, keyboard, monitor, HDMI to micro HDMI cable, and a USB hub.
  - You can also connect your AWS DeepLens to a personal computer via SSH. For more information, see How to Connect Your Device to Your Home or Office Wi-Fi Network When the Wi-Fi SSID or Password Contains Special Characters? (p. 116).

Note
It is possible to use a micro SD with a USB-based card reader, but this is not recommended. A factory reset cannot be initiated if the card slot on the back of the AWS DeepLens device is in use.

Preparation

You must complete the procedure in this section before performing a factory reset. At a high level, the preparation process includes the following.

- Formatting a USB flash drive into the following two partitions:
  - 1st partition: FAT32 of 2 gb
  - 2nd partition: NTFS of at least 9 gb
- Making the USB flash drive bootable:
  - Download the required customized Ubuntu ISO image required for both 1.0 and 1.1, of AWS DeepLens.
  - Use the downloaded image to turn the first partition of your flash drive into a bootable device.
- Copy the factory restore files on a USB drive:
  - Download the compressed factory restore package for your version of AWS DeepLens:
    - AWS DeepLens v1.0
    - AWS DeepLens v1.1.
  - Unzip the package and put the unpacked files onto the 2nd partition (formatted as NTFS) of the USB drive.

You only do this once to set up your USB flash drive. After that, you can use the same flash drive to reset your AWS DeepLens as needed.

There are multiple ways to partition and format a USB drive. Depending on the computer you use, specific tasks may differ from one operating system to another.

The following procedure requires that you have set up your AWS DeepLens device as an Ubuntu computer and uses two third-party applications, GParted and UNetbootin. GParted is a partition-editing application and UNetbootin creates bootable USB drives.

The same instructions apply if you are using a personal computer running the Ubuntu operating system.

To partition a USB drive and make it bootable by using an Ubuntu computer

1. Open an Ubuntu terminal window and run the following commands to install and launch GParted.

```
sudo apt-get update; sudo apt-get install gparted
gparted
```

2. Open the GParted console.
3. In the GParted console, choose /dev/sda from the drop-down menu in the upper-right corner, and then delete any existing partitions.

4. Next, delete any existing partitions.

5. To create the FAT32 partition, choose the file icon and then set the parameters as follows.

   - **Free space preceding:** 1
   - **New size:** 2048
   - **Free space following:** 28551
   - **Align to:** MiB
   - **Create as:** Primary Partition
   - **Partition name:**
   - **File system:** fat32
   - **Label:** BOOT
6. Then, choose Add.
7. To create the NTFS partition, choose the file icon and then set the parameters as follows.

   Free space preceding: 0

   New size: 28551

   Free space following: 0

   Align to: MiB

   Create as: Primary Partition

   Partition name:

   File system: ntfs

   Label: Flash

8. Then, choose Add.

After successfully partitioning your USB drive into the FATS32 and NTFS partitions, the USB drive partitions will appear in the GParted console.
Preparing to perform factory reset on your AWS DeepLens device

Now you are ready to make the partitioned USB drive bootable using UNetbootin.

To make a USB drive bootable using UNetbootin

1. Download the customized Ubuntu ISO image.
2. Open an Ubuntu terminal window.
3. Run the following commands to install and launch Unetbootin.

   ```
   sudo apt-get update; sudo apt-get install unetbootin
   sudo unetbootin
   ```

4. In the UNetbootin window choose Diskimage.
5. Then, choose ISO.
6. Next, choose the... to open the file explorer.
7. Then, choose the customized Ubuntu ISO file you downloaded previously.
8. For Type, choose USB Drive.
9. For Drive, choose /dev/sda1.
10. Then, choose OK.
Preparing to perform factory reset on your AWS DeepLens device

Note
The customized Ubuntu image might be more recent than what's shown here. If it is, use the most recent version of the Ubuntu image.

Now that you have successfully created a bootable USB drive. Use the procedure below to copy the factory restore files to the NTFS partition of your USB drive.

Note
You must use the factory restore package associated with the correct version of your AWS DeepLens device.

To copy the factory restore files to the NTFS partition of your USB drive

1. Download the compressed factory restore package for your version of AWS DeepLens.
   - AWS DeepLens v1.0
   - AWS DeepLens v1.1

2. Unzip the downloaded package.
   ```
   unzip your-file-name.zip
   ```

3. Copy the following uncompressed files to the second (NTFS) partition of the USB drive:

   **For AWS DeepLens v1.0**
   
   *Image files*
   - DeepLens_image_1.3.22.bin
   - DeepLens_1.3.22.md5

   *Script file*
After completing these procedures you should have successfully partitioned your USB flash drive into two partitions and added the necessary files to each partition.

**Using a partitioned USB drive to restore your AWS DeepLens device**

Follow the instructions to restore your AWS DeepLens device to its factory settings. The procedures below assume you have successfully completed the steps outlined in the section called “Preparing to perform factory reset on your AWS DeepLens device” (p. 100).

These instructions require you to connect your AWS DeepLens device to a monitor and keyboard.

**Warning**

All data previously stored on your AWS DeepLens device will be erased.

**To restore your AWS DeepLens device to its factory settings**

1. Insert the prepared USB drive into your AWS DeepLens device and power it on. Repeatedly press the **ESC** key to enter BIOS.
2. From the BIOS window on your monitor, choose **Boot From File**.
3. Then choose **USB VOLUME**.
4. Then choose **EFI**.
5. Then choose **BOOT**.
6. Then choose **BOOTx64.EFI**.
7. Next, your AWS DeepLens device reset will start automatically.

This occurs when the power LED indicator starts to flash and a terminal window pops up to display your progress. No further user input is necessary at this point.

**Note**

If an error occurs and the recovery fails, restart the procedure from step 1. For detailed error messages, see the **result.log** file that’s generated on the USB flash drive.

8. After the power LED light stops flashing and the terminal closes, signaling that the factory reset is complete. The device then reboots itself automatically.

Your device is now restored. You can disconnect your USB flash drive from AWS DeepLens.
Logging and Troubleshooting Your AWS DeepLens Project

AWS DeepLens Project Logs

When you create a new project, AWS DeepLens automatically configures AWS IoT Greengrass Logs. AWS IoT Greengrass Logs writes logs to Amazon CloudWatch Logs and to the local file system of your device. When a project is running, AWS DeepLens sends diagnostic messages to CloudWatch Logs as AWS IoT Greengrass log streams and to your AWS DeepLens device as local file system logs. The messages sent to CloudWatch Logs and your local file system logs are identical, except that the crash.log file is available only in file system logs.

CloudWatch Logs Log Groups for AWS DeepLens

CloudWatch Logs log events for AWS DeepLens are organized into the following log groups.

<table>
<thead>
<tr>
<th>Log Group</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>aws/greengrass/GreengrassSystem/certmanager</td>
<td>Diagnostic logs for certificate management</td>
</tr>
<tr>
<td>aws/greengrass/GreengrassSystem/connection_manager</td>
<td>Diagnostic logs for device connection management, including Lambda function configuration</td>
</tr>
<tr>
<td>aws/greengrass/GreengrassSystem/ip_detector</td>
<td>Diagnostic logs for IP address detection</td>
</tr>
<tr>
<td>aws/greengrass/GreengrassSystem/python_runtime</td>
<td>Diagnostic logs related to the Python runtime</td>
</tr>
<tr>
<td>aws/greengrass/GreengrassSystem/router</td>
<td>Diagnostic logs that are created when the results of inference are forwarded to AWS IoT</td>
</tr>
<tr>
<td>aws/greengrass/GreengrassSystem/runtime</td>
<td>Diagnostic logs related to the AWS IoT Greengrass runtime, for example, for (Message Queuing Telemetry Transport (MQTT) event subscription</td>
</tr>
</tbody>
</table>
Log Group | Contents
--- | ---
aws/greengrass/GreengrassSystem/spectre | Diagnostic logs related to the local shadow of AWS IoT
aws/greengrass/GreengrassSystem/syncmanager | Diagnostic logs for the device's AWS IoT topic subscription
aws/greengrass/GreengrassSystem/tes | Diagnostic logs related to provisioning IAM credentials for calling a Lambda function
aws/greengrass/Lambda/\textit{lambda\_function\_name} | Diagnostic logs reported by the specified Lambda inference function of your AWS DeepLens project

For more information about CloudWatch Logs, including access role and permissions requirements and limitations, see [CloudWatch Logs](#) in the [AWS IoT Greengrass Developer Guide](#).

**File System Logs for AWS DeepLens**

AWS IoT Greengrass Logs for AWS DeepLens are also stored in the local file system on your AWS DeepLens device. The local file system logs include the crash log, which is not available in CloudWatch Logs.

You can find the local file system logs in the following directories on your AWS DeepLens device.

<table>
<thead>
<tr>
<th>Log Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/awscam/greengrass/ggc/var/log</td>
<td>The top-level directory for the AWS IoT Greengrass logs for AWS DeepLens. The crash logs are in the \texttt{crash.log} file in this directory.</td>
</tr>
<tr>
<td>/opt/awscam/greengrass/ggc/var/log/system</td>
<td>The subdirectory that contains the AWS IoT Greengrass system component logs.</td>
</tr>
<tr>
<td>/opt/awscam/greengrass/ggc/var/log/user</td>
<td>The subdirectory that contains logs for user-defined Lambda inference functions.</td>
</tr>
</tbody>
</table>

For more information about AWS IoT Greengrass file system logs for AWS DeepLens, including access requirements, see [File System Logs](#) in the [AWS IoT Greengrass Developer Guide](#).
Troubleshooting AWS DeepLens

Use the following guidelines to troubleshoot issues with AWS DeepLens.

Topics

- Troubleshooting AWS DeepLens Software Issues (p. 109)
- Troubleshooting Device Registration Issues (p. 114)
- Troubleshooting Issues with Model Deployments to the AWS DeepLens Device (p. 120)

Troubleshooting AWS DeepLens Software Issues

The following troubleshooting tips explain how to resolve issues that you might encounter with AWS DeepLens software.

Topics

- How to handle an import error – undefined symbol? (p. 109)
- How to Determine Which Version of AWS DeepLens Software You Have? (p. 110)
- How to Check the Latest Version of the awscam Software Package? (p. 110)
- How to Reactivate Wi-Fi Hotspots After Restarting the Device? (p. 111)
- How to Ensure That a Successfully Deployed Lambda Inference Function Can Be Called? (p. 111)
- How to Update the awscam Software Package to the Latest Version? (p. 111)
- How to Upgrade the awscam Software Package Dependencies? (p. 112)
- How to Install Security Updates on the Device? (p. 113)
- How to Handle Unsupported Architecture During a Device Update? (p. 114)

How to handle an import error – undefined symbol?

When writing a custom AWS Lambda inference function, if you import the awscam module prior to the cv2 module you will get an error like the following:

```python
File "my_lambda_detector.py", line 5, in import awscam
File "/usr/lib/python2.7/dist-packages/awscam/__init__.py", line 1, in from .model import *
File "/usr/lib/python2.7/dist-packages/awscam/model.py", line 14, in from awscamdldt import getLastFrame
ImportError: /opt/awscam/intel/deeplearning_deploymenttoolkit/deployment_tools/inference_engine/lib/intel64/libinference_engine.so: undefined symbol: _ZN3tbb10interface78internal15task_arena_base24internal_max_concurrencyEPKNS0_10task_arenaE
```

To resolve the error, you need to update the order of the imported modules in your import statement. Make sure that you are importing the awscam module prior to the cv2 module.
How to Determine Which Version of AWS DeepLens Software You Have?

The software on the AWS DeepLens device is a Debian package named awscam. To find the version of awscam that you have, you can use the AWS DeepLens console or the terminal on your AWS DeepLens device.

To use the AWS DeepLens console

1. Sign in to the AWS DeepLens console.
2. In the navigation pane, choose Devices.
3. In the Devices list, choose your registered device.

To use the terminal on your AWS DeepLens device

1. Connect your device to a monitor using a micro-HDMI cable, mouse, and keyboard or connect to the device using an ssh command.
2. In a terminal on the device, run the following command:

   ```
   dpkg -l awscam
   ```

3. Look for the version number in the version column. For example, in the following example, the installed version of awscam is 1.2.3.

   ```
   Desired=Unknown/Install/Remove/Purge/Hold
   | Status=Not/Inst/Conf-files/Unpacked/half-inst/trig-aWait/Trig-pend
   |/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
   +/-----------------------------------------------------------+
   | Name           Version     Architecture    Description
   |----------------------------------------------------------|
   |ii  awscam         1.2.3      amd64           awscam
   ```

How to Check the Latest Version of the awscam Software Package?

You can use the terminal on your AWS DeepLens device to see what the latest version of awscam is.

To see what the latest version of awscam is using your AWS DeepLens device

1. Connect to your AWS DeepLens device.
2. Open a terminal on your device.
3. Run the following commands:

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-cache policy awscam
   ```

   The following example shows an example output, where 1.2.3 would be the latest version of awscam on your device:
How to Reactivate Wi-Fi Hotspots After Restarting the Device?

If your device loses Wi-Fi connection and restarting your device doesn't reactivate Wi-Fi hotspots, you might be affected by the Linux kernel upgrade from Ubuntu. To resolve this, roll back the kernel.

To roll back the Linux kernel on your device

1. Open a terminal on your device.
2. Run the following command:
   ```
   ifconfig
   ```
3. Inspect the output of the command. If the output lists only the localhost network interface, turn off the device and then turn it back on to restart the system.
4. If you still don't have Wi-Fi access, run the following command to check which version of the Linux kernel is installed.
   ```
   uname -r
   ```
5. If you have the 4.13.x-xx version of the kernel, you are affected by the kernel upgrade from Ubuntu. To resolve this, roll back the kernel using the following commands. Replace x-xx with your version number:
   ```
   sudo apt remove linux-image-4.13.x-xx-generic linux-headers-4.13.x-xx-generic
   sudo reboot
   ```

   After the device has restarted, the kernel version should be 4.10.17+ or 4.13.x-xx-deeplens.

If the version of your awscam software is 1.2.0 or later, you shouldn't have this issue.

How to Ensure That a Successfully Deployed Lambda Inference Function Can Be Called?

If you successfully deployed an inference function to Lambda before January 10, 2018, but the Lambda function doesn't appear to be called to perform inference, and your Linux kernel version is 4.13.0-26, you are affected by the Linux kernel upgrade from Ubuntu. To resolve this, follow the procedure in How to Determine Which Version of AWS DeepLens Software You Have? (p. 110) to roll back the Linux kernel to Ubuntu 4.10.17+.

How to Update the awscam Software Package to the Latest Version?

If you enabled automatic updates when you set up your device, AWS DeepLens automatically updates awscam every time you turn on your device. If you find the software is out-of-date, restart the AWS DeepLens device and wait for a few minutes after the system is running.

The update might get delayed or fail under the following conditions:

- Scenario 1: The Ubuntu system is updated every time you restart the device. This blocks concurrent awscam automatic updates. To check if an Ubuntu update is running, run the following command from a terminal:
sudo lsof /var/lib/dpkg/lock

If the output looks similar to the following, a concurrent Ubuntu update is running:

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE/OFF</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>unattended</td>
<td>2638</td>
<td>root</td>
<td>4uW</td>
<td>REG</td>
<td>179,2</td>
<td>0</td>
<td>21</td>
<td>/var/lib/dpkg/lock</td>
</tr>
</tbody>
</table>

In this case, wait for the Ubuntu update to finish. If the installed version of awscam is earlier than 1.1.11, restart the system after Ubuntu finishes updating. Otherwise, wait for the awscam update to start automatically.

- Scenario 2: awscam installation can be interrupted by a system restart or other events. If this happens, awscam might be only partially configured. Run the following command to check the package version:

dpkg -l awscam

If the upgrade has not completed successfully, you see output similar to the following:

```
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-inst/trig-aWait/Trig-pend
| Err?=none|Reinst-required (Status,Err: uppercase=bad)
|/| Name Version Architecture Description
+++-==============-===========-==============-===============
iF  awscam         1.1.10      amd64          awscam
```

A status of `iF` prevents an awscam update. To resolve this issue, run the following command:

```
sudo dpkg --configure -a
```

Verify the status again and restart the device to let the automatic update of awscam proceed.

- Scenario 3: If you’ve tried the suggestions for Scenario 1 and 2, and awscam still hasn’t been updated, manually start the update by running the following commands:

```
sudo apt-get update
sudo apt-get install awscam
```

Allow several minutes for the update to finish. If AWS DeepLens reports an error during the upgrade process, see How to Upgrade the awscam Software Package Dependencies? (p. 112).

### How to Upgrade the awscam Software Package Dependencies?

When upgrading awscam on your device, you might get an error message about unmet dependencies. An example of such error message is shown in the following output:

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
You might want to run 'apt-get -f install' to correct these.
The following packages have unmet dependencies:
pulseaudio : Depends: libpulse0 (= 1:8.0-0ubuntu3.3) but 1:8.0-0ubuntu3.4 is installed
pulseaudio-module-bluetooth : Depends: pulseaudio (= 1:8.0-0ubuntu3.4)
pulseaudio-module-x11 : Depends: pulseaudio (= 1:8.0-0ubuntu3.4)
```
**Troubleshooting Software on Device**

**E: Unmet dependencies. Try using -f.**

To resolve such an error, run the following command from a terminal on your device:

```
sudo apt-get -f install
```

If the error persists or you get another error message similar to the following, you might need to force installation:

```
Errors were encountered while processing:
/var/cache/apt/archives/pulseaudio_1%3a8.0-0ubuntu3.4_amd64.deb
E: Sub-process /usr/bin/dpkg returned an error code (1)
```

To force installation, run the following commands:

```
sudo dpkg --configure -a
sudo dpkg -i --force-overwrite /var/cache/apt/archives/pulseaudio_1%3a8.0-0ubuntu3.4_amd64.deb
```

If you have the Linux kernel version 4.13-32, you might need to change the path of the pulse audio package to `/var/cache/apt/archives/pulseaudio_1%3a8.0-0ubuntu3.7_amd64.deb` in the preceding command.

Make sure that the package is installed by inspecting the output of the following command:

```
sudo apt-get -f install
```

If multiple packages show the `Errors were encountered while processing` error message, run the following command on each of them:

```
dpkg -i --force-overwrite
```

After forced installation has finished, run the following command to complete the upgrade:

```
sudo apt-get upgrade
```

**How to Install Security Updates on the Device?**

When using `ssh` to connect to your device, you might see messages like 245 packages can be updated and 145 updates are security updates.

In general, security updates don't affect the operation of your device. However, if you have security concerns, you can manually apply security updates with the following command:

```
sudo apt-get update
sudo apt-get upgrade
```

To update all packages at once, run the following command:

```
sudo apt-get dist-upgrade
```
If you get unmet dependencies error messages, follow the instruction in How to Upgrade the awscam Software Package Dependencies? (p. 112) to resolve the errors.

**How to Handle Unsupported Architecture During a Device Update?**

If you run the `sudo apt-get update` command and get the The https://awsdeepupdate.us-east-1.amazonaws.com packages repository is not set to public (access denied) causing error: "doesn't support architecture i386" error message, you can safely ignore it. The awscam package is supported only for x86_64 architecture.

**Troubleshooting Device Registration Issues**

Use the following guidelines to troubleshoot issues with AWS DeepLens device registration.

**Topics**
- Why Does My Attempt to Use the AWS DeepLens Console to Register a Device Go into an Apparently Endless Loop and Fail to Complete? (p. 114)
- My AWS DeepLens 2019 Edition(v1.1) Device Isn't Detected During Registration (p. 115)
- How to Perform a First-Time Update on a AWS DeepLens v1.1 Device (p. 115)
- How to Turn your Device Back to its Setup Mode to Complete Device Registration or Update Device Settings? (p. 116)
- How to Connect Your Device to Your Home or Office Wi-Fi Network When the Wi-Fi SSID or Password Contains Special Characters? (p. 116)
- What IAM Roles to Choose When None Is Available? (p. 118)
- How to View Project Output in the Chrome Browser on Mac El Capitan or Earlier? (p. 118)
- How to Fix an Incomplete Certificate (.zip) File? (p. 118)
- How to Fix an Incorrectly Uploaded Certificate File? (p. 119)
- How to Resolve the Maximum User Limits Exceeded Restriction for Devices, Projects, or Models? (p. 119)
- How to Fix Failed Deregistration of the AWS DeepLens Device? (p. 119)
- How to Resolve Failed Registration of the AWS DeepLens Device? (p. 119)
- How to Open the Device Setup Page When the Device's Local IP Address (192.168.0.1) Is Not Accessible? (p. 119)
- How to Make the Device's Wi-Fi Network Visible on Your Computer When the Device Wi-Fi Indicator Is Blinking or After Your Computer Has Connected to the Device? (p. 120)
- How to Fix an Unsuccessful Device Wi-Fi Reset? (p. 120)

**Why Does My Attempt to Use the AWS DeepLens Console to Register a Device Go into an Apparently Endless Loop and Fail to Complete?**

When you use the AWS DeepLens console to register a device, if the registration fails to complete after you choose Register device, you may have used an unsupported browser. Make sure that you do not use the following browser:

**Unsupported Browser for the AWS DeepLens Console**
- Internet Explorer 11 on Windows 7
My AWS DeepLens 2019 Edition(v1.1) Device Isn't Detected During Registration

When registering your AWS DeepLens 2019 Edition(v1.1) device, your computer might not detect the device after you've connected it to your computer with a USB cable. This prevents completing registration.

To ensure that your device can be detected, make sure that:

• Your device is powered on.
• Your computer is connected to the device through the REGISTRATION USB port at the bottom.
• Your computer isn't connected to Ethernet and a VPN network.
• Your firewall isn't blocking the AWS DeepLens network connection.
• You're using Chrome, Firefox, or Safari and have installed the latest operating system update.

If your computer still doesn't detect your device, disconnect the USB cable from the REGISTRATION USB port on the device, reconnect it, and wait for a couple of minutes.

If that doesn't work, check the network interface service order on your computer. The network interface service order can prevent your device from being detected during registration. For example, if the USB-C interface has a higher preference over the standard USB interface on your computer, your computer could default to the USB-C port to scan attached USB devices. As a result, your AWS DeepLens device would be invisible to your computer. In this case, reorder the preference of network types. To do so, see How to prioritize which internet connection your Mac uses or How to change the priority order of network adapters on Windows 10.

How to Perform a First-Time Update on a AWS DeepLens v1.1 Device

If you have a AWS DeepLens 2019 (v1.1) device shipped before 3/28/2020 and it is not running software version v1.4.5, you may need to perform a one-time software update.

To perform the update, you will need:

• A small paperclip or pin to reset the device
• AWS DeepLens 2019 (v1.1) device and power supply

To perform a first-time update:

1. Plug in your AWS DeepLens device.
2. On the back of the AWS DeepLens device, insert a paper clip or pin into the reset pinhole. After you hear a click, wait about 20 seconds for the Wi-Fi indicator (middle light) to blink.

   When the Wi-Fi indicator blinks, your device is in setup mode.
4. In the AWS DeepLens console, select Register device.
5. Select HW v1.

   Warning
   You must select HW v1 even though your device is v1.1.
6. Provide a name your AWS DeepLens device. select Download the certificates. to download the certificates onto your computer.
7. Select **Download the certificates** to download the certificates onto your computer.

8. Follow the instructions on screen to connect to the AWS DeepLens Wi-Fi network and continue the registration process.

9. Once you've complete the registration process, you will see a notice inside the device details page stating that an update is available for your device. Scroll down to the bottom click **Update**.

   **Note**
   
   It can take 10 mins for your device to update.

10. When the update has completed, the device will restart. When the device goes back online, it will be updated to v1.4.5.

Once your AWS DeepLens device is updated to v1.4.5, you can use the USB cable for future updates.

### How to Turn your Device Back to its Setup Mode to Complete Device Registration or Update Device Settings?

If you don't see your device's Wi-Fi network SSID among the available Wi-Fi networks on your computer and the device's Wi-Fi indicator (the middle LED light) does not blink, you cannot connect to the device to set up the device and to complete the registration.

Your device is in its setup mode when the Wi-Fi indicator (the middle LED light) on the front of the device blinks. When you start registering your device, the device is booted into the setup mode after you power it on. Only in the setup mode is the device's Wi-Fi (AMDC-NNNN) network visible in the list of available Wi-Fi networks on your computer. After 30 minutes, the device exits the setup mode, and the Wi-Fi indicator stays on and stops blinking.

Your device must be in the setup mode for you to connect your computer to the device, to configure the device to complete the registration or to update the device settings, or to view the output of a deployed project. If you don't finish the setup within the allotted time, you must reset the device back to its setup mode and then reconnect your computer to the device's Wi-Fi network.

After connecting your computer to the device's Wi-Fi network, navigate to `http://deeplens.config` from a web browser to open the device configuration page and to complete setting up your device. For an initial registration, you may want type `http://deeplens.amazon.net` in the browser's address bar to open the configuration page.

For detailed instructions to connect to your device's Wi-Fi network, see the section called “Connect to Device” (p. 23).

### How to Connect Your Device to Your Home or Office Wi-Fi Network When the Wi-Fi SSID or Password Contains Special Characters?

If your home or office network Wi-Fi name (SSID) or password contains special characters (including single quotes, backslashes, or white spaces), you might not be able to connect your AWS DeepLens device to the home or office Wi-Fi network when setting up your device on the device configuration page (`http://deeplens.amazon.net` or `http://deeplens.config`).

To work around this, follow the steps below to use SSH commands to log into the device and connect it to your home or office Wi-Fi network.

**To connect your DeepLens device to your home or office Wi-Fi network when the Wi-Fi SSID and password contains special characters**

1. Connect to your device's Wi-Fi network.
Troubleshooting Registration of Device

a. Power on your DeepLens and press the power button on the front to turn on the device. Skip this step if the device is already turned on.

b. Wait until the device enters into the setup mode when the Wi-Fi indicator on the front of the device starts to flash. If you skipped the previous step, you can turn the device into its setup mode by pressing a paper clip into the reset pinhole on the back of the device and, after feeling a click, wait for about 20 seconds for the Wi-Fi indicator to blink.

c. Connect your computer to the device's Wi-Fi network by selecting the device Wi-Fi network SSID (of the AMDC-NNNN format) from the list of available networks and type the network password. The SSID and password are printed on the bottom of your device. On a Windows computer, choose Connecting using a security key instead when prompted for Enter the PIN from the router label (usually 8 digits).

2. After the Wi-Fi connection is established, open a web browser on your computer and type http://deeplens.amazon.net/#deviceAccess in the address bar.

3. In the Configure device access page, choose Enable under SSH server. Create a device password if you haven't already done so. Choose Save.

   **Important**
   After choosing Save do not choose Finish. Otherwise, you'll be disconnected from the device and can't proceed in the following step.
   If you've chosen Finish, follow Step 1-3 above to get back to the device's Wi-Fi network before continuing to the next step.

4. While your computer is connected to the device (AMDC-NNNN) network Wi-Fi connection, open a terminal on your computer and run the following SSH command to log in to your device:

   ```
   ssh aws_cam@deeplens.amazon.net
   ```

   Type the device password.

   **Note**
   On a computer running Windows, you can use PuTTY or a similar SSH client to execute the SSH command.

5. After you have logged in, run the following shell command in the terminal:

   ```
   sudo nmcli device wifi con '<wifi_ssid>' password '<wifi_password>' ifname mlan0
   ```

   Replace <wifi_ssid> and <wifi_password> with the SSID and the password for the Wi-Fi connection, respectively.

   You must enclose the SSID and password in single quotes. If the SSID or password contains a single quote, escape each instance by prefixing a back slash (\) and enclosing them within a pair of single quotes. For example, if a single quote appears in the original <wifi_ssid> as Jane's Home Network, the escaped version is Jane\'s Home Network.

   After the command has run, verify that your device is connected to the internet by pinging any public website.

6. Go to http://deeplens.amazon.net or http://deeplens.config on your browser to continue setting up the device, as prescribed by Step 3.b in Set Up Your Device (p. 27).

   When prompted, update the device software to version 1.3.10 or higher. The update ensures that your AWS DeepLens device can connect to your home or office Wi-Fi network from the AWS DeepLens console so you won't have to repeat this workaround.
What IAM Roles to Choose When None Is Available?

If the required IAM roles are not available in your account when you register your device using the AWS DeepLens console for the first, you will be prompted to create the roles with a single click of button.

How to View Project Output in the Chrome Browser on Mac El Capitan or Earlier?

On a Mac computer (El Capitan and earlier), you must provide a password to upload the streaming certificate into the key chain while using Chrome. To use Chrome to view project output streamed from your device, you must update the device software to associate the password of DeepLens with the certificate first and then use the password to add the streaming certificate to the key chain. The steps are detailed in the following procedure.

To set up the DeepLens password on the device to enable viewing the project output in Chrome on Mac El Capitan or earlier

1. Update the device software to set up the DeepLens password for the streaming certificate:
   a. Connect to your AWS DeepLens device using an SSH or uHDMI connection.
   b. On the device terminal, type `$wget https://s3.amazonaws.com/cert-fix/cert_fix.zip`
   c. Type `$unzip cert_fix.zip` to unzip the file.
   d. Type `$cd cert_fix` to step into the unzipped directory.
   e. Type `$sudo bash install.s` to install the updates.
   f. Restart your device.
2. After the device is started, upload the streaming certificate to your Mac (El Capitan or earlier) for viewing project output:
   a. Connect your computer to the devices Wi-Fi (AMDC-NNNN) network
   b. Open the device setup page in your browser using the deeplens.config URL
   c. Choose Enable streaming certificates. Ignore the browser instructions.
   d. Choose the Download streaming certificates button.
   e. After the certificates are downloaded, rename the downloaded certificates from download to my_device.p12 or some_other_unique_string.p12.
   f. Double click on your certificate to upload it into the key chain.
   g. The key chain will ask you for a certificate password, enter DeepLens.
   h. To view the project output streamed from your device, open Chrome on your Mac computer and navigate to your device's video server web page at `https://your_device_ip:4000` or use the AWS DeepLens console to open the page.

   You’ll be asked to select a streaming certificate from the key chain. However, the key chain refers to any streaming certificate uploaded in Step 2.f above as client_cert. To differentiate any multiple like-named key-chain entries, use the expiration date and validation date when choosing the streaming certificate.
   i. Add the security exception. When prompted, enter your computer system's username and password, and choose to have the browser remember it so you don’t have to keep entering it.

How to Fix an Incomplete Certificate (.zip) File?

If you download a certificate .zip file and forget to choose the Finish button, you get an incomplete and, therefore, unusable certificate file. To fix this, delete the downloaded zip file and reregister your device.
How to Fix an Incorrectly Uploaded Certificate File?

If you accidentally uploaded an incorrect certificate (.zip) file, upload the correct certificate (.zip) file to overwrite the incorrect one.

How to Resolve the Maximum User Limits Exceeded Restriction for Devices, Projects, or Models?

Deregister the device, delete a project, or delete a model before adding new one.

How to Fix Failed Deregistration of the AWS DeepLens Device?

Stop deregistration and reregister the device.

To stop deregistering and then reregister an AWS DeepLens device

1. Turn the device back to its setup mode by inserting a small paper clip into the reset pinhole at the back of the device.
2. Reregister the device with a new device name.
3. Upload the new certificate to replace the old one.

How to Resolve Failed Registration of the AWS DeepLens Device?

Device registration often fails because you have incorrect or insufficient permissions. Make sure that the correct IAM roles and permissions are set for the AWS services you use.

For example, when setting the permissions in the AWS DeepLens console, you must already have created an IAM role with the required permissions for AWS IoT Greengrass and associated this role with the IAM role for AWS Greengrass option. If registration fails, make sure that you've created and specified the correct roles, then reregister the device.

Specifying an existing Lambda role for the IAM role for AWS Lambda can also cause registration to fail if the role name doesn't start with AWSDeepLens. Specifying a role whose name doesn't begin with AWSDeepLens doesn't affect the deployment of Lambda functions.

To set up the roles correctly, follow the instructions in Register Your AWS DeepLens Device (p. 9) and check with the AWS DeepLens console tips for each role.

How to Open the Device Setup Page When the Device's Local IP Address (192.168.0.1) Is Not Accessible?

If your AWS DeepLens device is running software (awscam) version 1.3.6 or later, you can open the device setup page by navigating to http://deeplens.amazon.net (the first time you register the device) or http://deeplens.config in a browser window on your computer. Your computer must be connected to the device's (AMDC-nnnn) Wi-Fi network (p. 23).

If your device is running an earlier version of the awscam package, update to the latest version by running the following commands from a terminal on the device:

```
sudo apt update
sudo apt install awscam
```
If you don’t want to update the awscam package to the latest version yet, you can navigate to http://192.168.0.1 to launch the device setup page if your AWS DeepLens device software package is older than 1.2.4 or you can navigate to http://10.105.168.217 if the device software package is 1.2.4 or newer.

If your device software is older than 1.2.4 and your home or office Wi-Fi network router also uses 192.168.0.1 as the default IP address, reset the router's IP address to, for example, 192.168.1.0. For instructions on resetting your router's IP address, see How do I change the IP Address of my router?

If your device's Wi-Fi network is unresponsive, reset the device and connect to it again. To reset the device, press a pin on the RESET button on the back of the device, and wait until the Wi-Fi indicator (on the front of the device) blinks.

**How to Make the Device's Wi-Fi Network Visible on Your Computer When the Device Wi-Fi Indicator Is Blinking or After Your Computer Has Connected to the Device?**

When you can’t see your device's Wi-Fi network on your laptop even though the middle LED light on the device is blinking or if your computer is still connected to the device Wi-Fi network after the middle LED light stops blinking, refresh the available Wi-Fi networks on your computer. Usually, this involves turning off the laptop Wi-Fi and turning it back on.

It takes up to 2 minutes to reboot a device and for the device Wi-Fi network to be ready to accept connection requests.

**How to Fix an Unsuccessful Device Wi-Fi Reset?**

If the device's Wi-Fi indicator (middle LED light) isn't blinking after you reset the device by pressing a pin into the reset pinhole on the back of it, connect the device to the internet with an Ethernet cable, connect the device to a monitor, a keyboard and a mouse, log in to the device, open a terminal window, and run the following commands to reset the awscam package:

```
sudo systemctl status softap.service
```

If the command returns error code 203, reinstall awscam-webserver by running the following commands on your AWS DeepLens device:

```
sudo apt-get install --reinstall awscam-webserver
sudo reboot
```

The successful reboot sets up the device's Wi-Fi network, and the middle LED light on the device will start to blink.

**Troubleshooting Issues with Model Deployments to the AWS DeepLens Device**

Use the following information to troubleshoot issues that occur when deploying models to an AWS DeepLens device.

**Topics**

- [How to Resolve an Access Denied Error Encountered While Downloading a Model After Device Registration Went through without Errors?](p. 121)
Troubleshooting Model Deployments to Device

- How to Resolve the ModelDownloadFailed Error? (p. 121)
- Resolve Model Optimization Failure Reported As std::bad_alloc() (p. 121)
- How to Resolve Model Optimization Failure Caused by a Missing stride Attribute? (p. 121)
- How to Resolve Model Optimization Failure When the List Object Is Missing the shape Attribute? (p. 122)
- How to Ensure Reasonable Inference for a Model? (p. 123)
- How to Determine Why AWS DeepLens Classifies Data Incorrectly When the Model Performs Well on the Validation Set? (p. 123)

How to Resolve an Access Denied Error Encountered While Downloading a Model After Device Registration Went through without Errors?

When setting permissions during device registration, make sure that you have the IAM role for AWS IoT Greengrass created and the role is associated with the IAM group role for AWS Greengrass option on the console when setting permissions during device registration. If you didn't, reregister the device with the correct roles.

How to Resolve the ModelDownloadFailed Error?

When using the AWS DeepLens console, you must provide two IAM roles for AWS IoT Greengrass: IAM Role for AWS Greengrass and IAM group role for AWS Greengrass. If you specify the same IAM role for both, you get this error. To fix it, specify AWSDeepLensGreengrassRole for the IAM Role for AWS Greengrass and AWSDeepLensGreengrassGroupRole for the IAM group role for AWS Greengrass.

Resolve Model Optimization Failure Reported As std::bad_alloc()

This occurs because the version of MXNet on the device doesn't match the version used to train the model. Upgrade the version of MXNet on the device by running the following command from a terminal on the device:

```bash
sudo pip3 install mxnet==1.0.0
```

We assume that the version of MXNet used for training is 1.0.0. If you use a different version for training, change the version number accordingly.

How to Resolve Model Optimization Failure Caused by a Missing stride Attribute?

If you haven't specified the stride argument in the hyper parameter list for pooling layers, the model optimizer fails and reports the following error message:

```
AttributeError: 'MxNetPoolingLayer' object has no attribute 'stride_x'
```

This occurs because the stride argument is removed from the latest MXNet pooling layers' hyper parameter list.

To fix the problem, add "stride": "(1, 1)" to the symbol file. In a text editor, edit your symbol file so that the pooling layer looks like this:

```python
{
```
"op": "Pooling",
"name": "pool1",
"attr": {
  "global_pool": "True",
  "kernel": "(7, 7)",
  "pool_type": "avg",
  "stride": "(1, 1)"
},
"inputs": <your input shape>
},

After the stride property is added to all the pooling layers, you should no longer get the error and everything should work as expected. For more information, see this forum post.

**How to Resolve Model Optimization Failure When the List Object Is Missing the shape Attribute?**

You receive the following error message during model optimization when the layer names for non-null operators have suffixes:

```python
File "/opt/intel/deeplearning_deploymenttoolkit_2017.1.0.5852/
deployment_tools/model_optimizer/model_optimizer_mxnet/mxnet_convertor/
mxnet_layer_utils.py", line 75, in transform_convolution_layer
res = np.ndarray(l.weights.shape)
AttributeError: 'list' object has no attribute 'shape'
```

In a text editor, open your model's symbol file (<model_name>-symbol.json). Remove suffixes from all of the layer names for non-null operators. The following is an example of how a non-null operator is defined:

```json
{
  "op": "Convolution",
  "name": "deep_dog_conv0_fwd",
  "attr": {
    "dilate": "(1, 1)",
    "kernel": "(3, 3)",
    "layout": "NCHW",
    "no_bias": "False",
    "num_filter": "64",
    "num_group": "1",
    "pad": "(0, 0)",
    "stride": "(2, 2)"
  }
}
```

Change "name": "deep_dog_conv0_fwd" to "name": "deep_dog_conv0".

In contrast, the following is an example of a null operator:

```json
{
  "op": "null",
  "name": "deep_dog_conv0_weight",
  "attr": {
    "__dtype__": "0",
    "__lr_mult__": "1.0",
    "__shape__": "(64, 0, 3, 3)",
    "__wd_mult__": "1.0"
  }
}
```
For a softmax layer, if the "attr": "{}" property is missing, add it to the JSON file. For example:

```json
{
    "op": "SoftmaxOutput",
    "name": "softmax",
    "attr": {},
    "inputs": [[[192,0,0]]]
}
```

Finally, make sure that you use only the supported layers in your model. For a list of supported MXNet layers, see [MXNet Models](p. 34).

**How to Ensure Reasonable Inference for a Model?**

To ensure reasonable inference based on a given model, the height and width of the model optimizer must match the height and width of images in the training set. For example, if you trained your model using images that are 512 pixels X 512 pixels, you must set your model optimizer's height and width to 512 X 512. Otherwise, the inference won't make sense.

**How to Determine Why AWS DeepLens Classifies Data Incorrectly When the Model Performs Well on the Validation Set?**

AWS DeepLens classifies data incorrectly even if the model performs well on a validation set when your training data wasn't normalized. Retrain the model with normalized training data.

If the training data has been normalized, also normalize the input data before passing it to the inference engine.
AWS DeepLens Device Library

The AWS DeepLens device library consists of a set of Python modules that provide objects and methods for various device operations:

- The awscam module for running inference code based on a project's model.
- The mo module for converting your Caffe, Apache MXNet or TensorFlow deep learning model artifacts into AWS DeepLens model artifacts and performing necessary optimization.
- The DeepLens_Kinesis_Video module for integrating with Kinesis Video Streams to manage streaming from the AWS DeepLens device to a Kinesis Video Streams stream.

Topics
- awscam Module for Inference (p. 124)
- Model Optimization (mo) Module (p. 130)
- DeepLens_Kinesis_Video Module for Amazon Kinesis Video Streams Integration (p. 139)

awscam Module for Inference

Use the awscam module to grab video frames from your AWS DeepLens device and load a deep learning model into the inference engine of the device. Use the model to run inference on captured image frames.

When you create an AWS Lambda inference function to use on your AWS DeepLens project, you use the awscam module. The awscam module requires the cv2 module. The cv2 module has a dependency on the awscam module, so you must import the awscam module before importing the cv2 module.

Topics
- awscam.getLastFrame Function (p. 124)
- Model Object (p. 125)

awscam.getLastFrame Function

Retrieves the latest frame from the video stream. The video streaming runs constantly when the AWS DeepLens is running.

Request Syntax

```python
import awscam
ret, video_frame = awscam.getLastFrame()
```

Parameters
- None

Return Type
- ret—A Boolean value (true or false) that indicates whether the call was successful.
- video_frame—A numpy.ndarray that represents a video frame.
Model Object

class awscam.Model

Represents an AWS DeepLens machine learning model.

```python
import awscam
model = awscam.Model(model_topology_file, loading_config, runtime)
```

Methods

- Model Class Constructor (p. 126)
- model.doInference Method (p. 127)
- model.parseResult Method (p. 129)
Model Class Constructor

Creates an awscam.Model object to run inference in a specific type of processor and a particular inference runtime. For models that are not Neo-compiled, the Model object exposes parsing the raw inference output in order to return model-specific inference results.

Request Syntax

```python
import awscam
model = awscam.Model(model_topology_file, loading_config, runtime=0)
```

Parameters

- **model_topology_file**—Required. When runtime=0, this parameter value is the path to an optimized model (.xml) file output by the `mo.optimize` method. When runtime=1, this parameter value is the name of the folder containing the compiled model artifacts, which include a .json file, a .params file, and a .so file.

  Neo-compiled models support only the Classification model type. Other models support Classification, Segmentation, and Single Shot MultiBox Detector (SSD).

  **Note**
  When deploying an SageMaker-trained SSD model, you must first run `deploy.py` (available from https://github.com/apache/incubator-mxnet/tree/v1.x/example/ssd/) to convert the model artifact into a deployable model. After cloning or downloading the MXNet repository, run the `git reset --hard 73d88974f8bca1e68441606fb0787a2cd17eb364` command before calling `deploy.py` to convert the model, if the latest version does not work.

- **loading_config** (dict)—Required. Specifies whether the model should be loaded into the GPU or CPU. The format of this parameter is a dictionary.

  **Valid values:**
  - {"GPU":1}—Loads the model into the GPU. To run inference in the Neo runtime (runtime=1), you must select GPU ("GPU":1).
  - {"GPU":0}—Loads the model into the CPU.
  - runtime int—Optional. Specifies the runtime to run inference in.

  **Valid values:**
  - 0—Intel DLDT as the default inference runtime.
  - 1—The Neo runtime to run inference on a compiled model.
model.doInference Method

Runs inference on a video frame (image file) by applying the loaded model. The method returns the result of the inference.

Request Syntax

```python
import awscam
model = awscam.Model(model_topology_file, loading_config)
raw_inference_results = model.doInference(video_frame)
```

Parameters

- `video_frame`—Required. A video frame from the AWS DeepLens video feeds.

Return Type

- `dict` — The inference result, as a dictionary of output layers based on the loaded model.

Returns

Returns a `dict` object with entries of key-value pairs. The key of an entry is the identifier of an output layer of the model. For the output of inference running in the default Intel DLDT runtime, the output layer identifier is the output layer name as specified in the model. For example, with MXNet, the output layer names are defined in the model's .json file. For the output of inference running in the Neo runtime, the output layer identifier is the ordinal number of the output layer as defined in the model. The value of an entry is a `list` object that holds the probabilities of the input `video_frame` over the labeled images used to train the model.

Example

Sample output:

Running inference in the Intel DLDT runtime on a model with an output layer named `SoftMax_67` of six labels, the inference outcome has the following format.

```json
{
    'SoftMax_67': array(
        [2.41881448e-08, 3.57339691e-09, 1.00263861e-07, 5.40415579e-09, 4.37702547e-04, 6.16787545e-08 ],
        dtype=float32)
}
```

If the Neo runtime (`runtime=1`) is used to run the inference, the raw inference result is a `dict` object, where `results[i]` holds the \(i^{th}\) output layer. For example, for an image classification network such as ResNet-50 with only one Softmax output layer, `results[0]` is a Numpy array with size \(N \times 1\) that gives the probability for each of the \(N\) labeled image types.

The following example output shows the raw inference result of the same model (above) running in the Neo runtime.
{
    "0": array([
        [2.41881448e-08,
         3.57339691e-09,
         1.00263861e-07,
         5.40415579e-09,
         4.37702547e-04,
         6.16787545e-08],
        dtype=float32)
    }
}
model.parseResult Method

Parses the raw inference results of some commonly used models, such as classification, SSD, and segmentation models, which are not compiled with Neo. For customized models, you write your own parsing functions.

Request Syntax

```python
import awscam
model = awscam.Model(model_topology_file, loading_config)
raw_infer_result = model.doInference(video_frame)
result = model.parseResult(model_type, raw_infer_result)
```

Parameters

- **model_type**—String that identifies the model type to use to generate the inference. Required.
  
  Valid values: classification, ssd, and segmentation

  **Note**
  When deploying an SageMaker-trained SSD model, you must first run `deploy.py` (available from [https://github.com/apache/incubator-mxnet/tree/v1.x/example/ssd/](https://github.com/apache/incubator-mxnet/tree/v1.x/example/ssd/)) to convert the model artifact into a deployable model. After cloning or downloading the MXNet repository, run the `git reset --hard 73d88974f8bca1e68441606fb9787a2cd17eb364` command before calling `deploy.py` to convert the model, if the latest version does not work.

- **raw_infer_result**—The output of the function `model.doInference(video_frame)`. Required.

Return Type

- **dict**

Returns

Returns a dict with a single entry of key-value pair. The key is the `model_type` value. The value is a list of `dict` objects. Each of the returned `dict` objects contains the probability calculated by the model for a specified label. For some model types, such as ssd, the returned `dict` object also contains other information, such as the location and size of the bounding box the inferred image object is located in.

Example

Sample output:
For the raw inference performed in the Intel DLDT runtime, the parsed inference result on a classification model type has the following format:

```json
{
   "classification": [
      {
         "label": "318", "prob": 0.5},
      {
         "label": "277", "prob": 0.3},
      ...
      {
         "label": "433", "prob": 0.001
      }
   ]
}
```

The corresponding parsed inference result on an ssd model type contains bounding box information and has the following format:

```json
{
}
```
Model Optimization (mo) Module

The mo Python module is a AWS DeepLens model optimization library that you can use to convert your Caffe, Apache MXNet, or TensorFlow\(^\text{(p. 34)}\) model artifacts to AWS DeepLens model artifacts and perform necessary optimization.

To optimize a model, call the mo.optimize function and specify the appropriate input parameters.

Topics

- mo.optimize Method (p. 130)
- Troubleshooting the Model Optimizer (p. 133)

mo.optimize Method

Converts AWS DeepLens model artifacts from a Caffe (.prototxt or .caffemodel), MXNet (.json and .params), or TensorFlow (.pb) representation to an AWS DeepLens representation and performs necessary optimization.

Syntax

```python
import mo
res = mo.optimize(model_name, input_width, input_height, platform, aux_inputs)
```

Request Parameters

- model_name: The name of the model to optimize.
  
  Type: string
  
  Required: Yes

- input_width: The width of the input image in pixels. The value must be a non-negative integer less than or equal to 1024.
  
  Type: integer.
  
  Required: Yes

- input_height: The height of the input image in pixels. The value must be a non-negative integer less than or equal to 1024.
  
  Type: integer.
  
  Required: Yes

- platform: The source platform for the optimization. For valid values, see the following table.
Type: string
Required: No

Valid platform Values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caffe or caffe</td>
<td>The optimization converts Caffe model artifacts (of the .prototxt or .caffemodel files) to AWS DeepLens model artifacts.</td>
</tr>
<tr>
<td>MXNet, mxNet or mx</td>
<td>The optimization converts Apache MXNet model artifacts (of the .json and .params files) to AWS DeepLens model artifacts. This is the default option.</td>
</tr>
<tr>
<td>TensorFlow or tensorflow or tf</td>
<td>The optimization converts TensorFlow model artifact (of the frozen graph .pb files) to AWS DeepLens model artifacts.</td>
</tr>
</tbody>
</table>

- aux_inputs: A Python dictionary object that contains auxiliary inputs, including entries common to all platforms and entries specific to individual platforms.

Type: Dict
Required: No

Valid aux_inputs dictionary Entries

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Applicable Platforms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--img-format</td>
<td>All</td>
<td>Image format. The default value is BGR.</td>
</tr>
<tr>
<td>--img-channels</td>
<td>All</td>
<td>Number of image channels. The default value is 3.</td>
</tr>
<tr>
<td>--precision</td>
<td>All</td>
<td>Image data type. The default value is FP16.</td>
</tr>
<tr>
<td>--fuse</td>
<td>All</td>
<td>A switch to turn on (ON) or off (OFF) fusing of linear operations to convolution. The default value is ON.</td>
</tr>
<tr>
<td>--models-dir</td>
<td>All</td>
<td>Model directory. The default directory is /opt/awscam/artifacts.</td>
</tr>
<tr>
<td>--output-dir</td>
<td>All</td>
<td>Output directory. The default directory is /opt/awscam/artifacts.</td>
</tr>
<tr>
<td>--input_proto</td>
<td>Caffe</td>
<td>The prototxt file path. The default value is an empty string (&quot;&quot;).</td>
</tr>
<tr>
<td>Item Name</td>
<td>Applicable Platforms</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--epoch</td>
<td>MXNet</td>
<td>Epoch number. The default value is 0.</td>
</tr>
<tr>
<td>--input_model_is_text</td>
<td>TensorFlow</td>
<td>A Boolean flag that indicates whether the input model file is in text protobuf format (True) or not (False). The default value is False.</td>
</tr>
</tbody>
</table>

Returns

The `optimize` function returns a result that contains the following:

- `model_path`: Path of the optimized model artifacts when they are successfully returned.
  
  Type: string

- `status`: Operational status of the function. For possible cause of failures and corrective actions when the method call fails, see the status table below.
  
  Type: integer

<table>
<thead>
<tr>
<th>status</th>
<th>Cause</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Model optimization succeeded.</td>
<td>No action needed.</td>
</tr>
<tr>
<td>1</td>
<td>Model optimization failed because the requested platform is not supported.</td>
<td>• Choose a supported platform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make sure that the platform name is spelled correctly.</td>
</tr>
<tr>
<td>2</td>
<td>Model optimization failed because you are using inconsistent platform versions.</td>
<td>• Make sure that you are running the latest version of the platform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To check your version, at a command prompt, run <code>pip install mxnet</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make sure that there are no unsupported layers in the model for the target platform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make sure that your awscam software is up-to-date.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• See [Troubleshooting the Model Optimizer (p. 133)] for recommended actions for error messages reported in the CloudWatch Logs for AWS DeepLens and on your AWS DeepLens device.</td>
</tr>
</tbody>
</table>

To load the optimized model for inference, call the `awscam.Model` API and specify the `model_path` returned from this function.
Troubleshooting the Model Optimizer

In this section, you'll find a list of frequently asked questions and answers about errors reported by the model optimizer. The AWS DeepLens model optimizer depends on the Intel Computer Vision SDK, which is installed with the AWS DeepLens software. For errors not covered here, see Intel Computer Vision SDK Support and ask a question on the forum.

Topics

- How to handle the "Current caffe.proto does not contain field." error? (p. 134)
- How to create a bare Caffe model with only prototxt? (p. 134)
- How to handle the "Unable to create ports for node with id." error? (p. 134)
- How to Handle "Invalid proto file: there is neither 'layer' nor 'layers' top-level messages." error? (p. 134)
- How to handle the "Old-style inputs (via 'input_dims') are not supported. Please specify inputs via 'input_shape'." error? (p. 134)
- How to handle the "Invalid prototxt file: value error." error? (p. 136)
- How to handle the "Error happened while constructing caffe.Net in the Caffe fallback function." error? (p. 136)
- How to handle the "Cannot infer shapes due to exception in Caffe." error? (p. 136)
- How to handle the "Cannot infer shape for node {} because there is no Caffe available. Please register python infer function for op or use Caffe for shape inference." error? (p. 136)
- How to handle the "Input shape is required to convert MXNet model. Please provide it with --input_width and --input_height." error? (p. 136)
- How to handle the "Cannot find prototxt file: for Caffe please specify --input_proto - a protobuf file that stores topology and --input_model that stores pretrained weights." error? (p. 137)
- How to handle the "Specified input model does not exist." error? (p. 137)
- How to handle the "Failed to create directory ... Permission denied!" error? (p. 137)
- How to handle the "Discovered data node without inputs and value." error? (p. 137)
- How to handle the "Placeholder node doesn't have input port, but input port was provided." error? (p. 137)
- How to handle the "No or multiple placeholders in the model, but only one shape is provided, cannot set it." error? (p. 137)
- How to handle the "Cannot write an event file for the tensorboard to directory." error? (p. 137)
- How to handle the "Stopped shape/value propagation at node." error? (p. 137)
- How to handle the "Module tensorflow was not found. Please install tensorflow 1.2 or higher." error? (p. 138)
- How to handle the "The following error happened while loading mxnet model ..." error? (p. 138)
- How to handle the "Cannot read the model file: it is incorrect TensorFlow model file or missing." error? (p. 138)
- How to handle the "Cannot pre-process TensorFlow graph after reading from model file. File is corrupt or has unsupported format." error? (p. 138)
- How to handle the "Input model name is not in an expected format, cannot extract iteration number." error? (p. 138)
- How to handle the "Cannot convert type of placeholder because not all of its outputs are 'Cast' to float operations." error? (p. 138)
- How to handle the "Data type is unsupported." error? (p. 138)
- How to handle the "No node with name ..." error? (p. 138)
- How to handle the "Module mxnet was not found. Please install mxnet 1.0.0" error? (p. 138)

133
• How to handle the "... elements of ... were clipped to infinity while converting a blob for node [...] to ..." error? (p. 139)
• How to handle the "... elements of ... were clipped to zero while converting a blob for node [...] to ..." error? (p. 139)
• How to handle the " topology contains no 'input' layers." error? (p. 139)

How to handle the "Current caffe.proto does not contain field." error?

Your model has custom layers that are not supported by the model optimizer.

How to create a bare Caffe model with only prototxt?

To create a bare Caffe model with only .prototxt, import the Caffe module and run the following:

```python3
import caffe
net = caffe.Net('PATH_TO_PROTOTXT/my_net.prototxt', caffe.TEST)
net.save('PATH_TO_PROTOTXT/my_net.caffemodel')
```

How to handle the "Unable to create ports for node with id." error?

Your model has custom layers that aren't supported by the model optimizer. Remove the custom layers.

How to Handle "Invalid proto file: there is neither 'layer' nor 'layers' top-level messages." error?

The structure of a Caffe topology is described in the caffe.proto file. For example, in the model optimizer you might find the following default proto file: /opt/awscom/intel/deeplearning_deploymenttoolkit/deployment_tools/model_optimizer/mo/front/caffe/proto/my_caffe.proto. This file contains the structure, for example:

```protobuf
message NetParameter {
  // ... some other parameters

  // The layers that make up the net. Each of their configurations, including
  // connectivity and behavior, is specified as a LayerParameter.
  repeated LayerParameter layer = 100;  // Use ID 100 so layers are printed last.

  // DEPRECATED: use 'layer' instead.
  repeated V1LayerParameter layers = 2;
}
```

This means that any topology should contain layers as top-level structures in prototxt. For more information, see LeNet topology.

How to handle the "Old-style inputs (via 'input_dims') are not supported. Please specify inputs via 'input_shape'." error?

The structure of a Caffe topology is described in the caffe.proto file. For example, in the model optimizer, you can find the following default proto file: /opt/awscom/intel/
deeplearning_deploymenttoolkit/deployment_tools/model_optimizer/mo/front/caffe/proto/my_caffe.proto. This file contains the structure, for example:

```protobuf
message NetParameter {
  optional string name = 1;  // Consider giving the network a name.
  // DEPRECATED. See InputParameter. The input blobs to the network.
  repeated string input = 3;
  // DEPRECATED. See InputParameter. The shape of the input blobs.
  repeated BlobShape input_shape = 8;

  // 4D input dimensions are deprecated. Use "input_shape" instead.
  // If specified, for each input blob, there should be four
  // values specifying the num, channels, and height and width of the input blob.
  // Therefore, there should be a total of (4 * #input) numbers.
  repeated int32 input_dim = 4;
  // ... other parameters
}
```

Specify the input layer of the provided model using one of the following formats:

1. **Input layer format 1:**

```protobuf
input: "data"
inpuinput_shape {
  dim: 1
  dim: 3
  dim: 227
  dim: 227
}
```

2. **Input layer format 2:**

```protobuf
input: "data"
inpuinput_shape {
  dim: 1
  dim: 3
  dim: 600
  dim: 1000
}
input: "im_info"
inpuinput_shape {
  dim: 1
  dim: 3
}
```

3. **Input layer format 3:**

```protobuf
layer {
  name: "data"
type: "Input"
top: "data"
  input_param {shape: {dim: 1 dim: 3 dim: 600 dim: 1000}}
}
layer {
  name: "im_info"
type: "Input"
```
4. Input layer format 4:

```
  input: "data"
  input_dim: 1
  input_dim: 3
  input_dim: 500
```

However, if your model contains more than one input layer, the model optimizer can convert the model with an input layer of format 1, 2, and 3. You can't use format 4 in any multi-input topology.

**How to handle the "Invalid prototxt file: value error." error?**

See the section called "How to Handle "Invalid proto file: there is neither 'layer' nor 'layers' top-level messages." error? " (p. 134) and the section called "How to handle the "Cannot find prototxt file: for Caffe please specify --input_proto - a protobuf file that stores topology and --input_model that stores pretrained weights." error? " (p. 137).

**How to handle the "Error happened while constructing caffe.Net in the Caffe fallback function." error?**

The model optimizer can't use the Caffe module to construct a net, while it is trying to infer a specified layer in the Caffe framework. Make sure that your .caffemodel and .prototxt files are correct. To make sure that the problem is not in the .prototxt file, see the section called "How to create a bare Caffe model with only prototxt?" (p. 134).

**How to handle the "Cannot infer shapes due to exception in Caffe." error?**

Your model has custom layers that are not supported by the model optimizer. Remove any custom layers.

**How to handle the "Cannot infer shape for node {} because there is no Caffe available. Please register python infer function for op or use Caffe for shape inference." error?**

Your model has custom layers that are not supported by the model optimizer. Remove any custom layers.

**How to handle the "Input shape is required to convert MXNet model. Please provide it with --input_width and --input_height." error?**

To convert a MXNet model to an IR, you must specify the input shape, because MXNet models do not contain information about input shapes. Use the --input_shape flag to specify the input_width and input_height.
How to handle the "Cannot find prototxt file: for Caffe please specify --input_proto - a protobuf file that stores topology and --input_model that stores pretrained weights." error?

The model optimizer can't find a prototxt file for a specified model. By default, the .prototxt file must be located in the same directory as the input model with the same name (except for the extension). If any of these conditions is not satisfied, use --input_proto to specify the path to the prototxt file.

How to handle the "Specified input model does not exist." error?

Most likely, you have specified an incorrect path to the model. Make sure that the path is correct and the file exists.

How to handle the "Failed to create directory ... Permission denied!" error?

The model optimizer can't create a directory specified as the -output_dir parameter. Make sure that you have permissions to create the specified directory.

How to handle the "Discovered data node without inputs and value." error?

One of the layers in the specified topology might not have inputs or values. Make sure that the provided .caffemodel and .protobuf files contain all required inputs and values.

How to handle the "Placeholder node doesn't have input port, but input port was provided." error?

You might have specified an input node for a placeholder node, but the model does not contain the input node. Make sure that the model has the input or use a model-supported input node.

How to handle the "No or multiple placeholders in the model, but only one shape is provided, cannot set it." error?

You might have provided only one shape for the placeholder node for a model that contains no inputs or multiple inputs. Make sure that you have provided the correct data for placeholder nodes.

How to handle the "Cannot write an event file for the tensorboard to directory." error?

The model optimizer failed to write an event file in the specified directory because that directory doesn't exist or you don't have permissions to write to it. Make sure that the directory exists and you have the required write permission.

How to handle the "Stopped shape/value propagation at node." error?

The model optimizer can't infer shapes or values for the specified node because: the inference function has a bug, the input nodes have incorrect values or shapes, or the input shapes are invalid. Verify that the inference function, input values, or shapes are correct.
How to handle the "Module tensorflow was not found. Please install tensorflow 1.2 or higher." error?

To use the model optimizer to convert TensorFlow models, install TensorFlow 1.2 or higher.

How to handle the "Cannot read the model file: it is incorrect TensorFlow model file or missing." error?

The model file should contain a TensorFlow graph snapshot of the binary format. Ensure that --input_model_is_text is provided for the model in the text format, by specifying the --input_model_is_text parameter as false. By default, a model is interpreted a binary file.

How to handle the "Cannot pre-process TensorFlow graph after reading from model file. File is corrupt or has unsupported format." error?

Make sure that you've specified the correct model file, the file has the correct format, and the content of the file isn't corrupted.

How to handle the "Input model name is not in an expected format, cannot extract iteration number." error?

MXNet model files must be in .json or .para format. Use the correct format.

How to handle the "Cannot convert type of placeholder because not all of its outputs are 'Cast' to float operations." error?

Use the FP32 data type for the model's placeholder node. Don't use UINT8 as the input data type for the placeholder node.

How to handle the "Data type is unsupported." error?

The model optimizer can't convert the model to the specified data type. Set the data type with the --precision parameter with FP16, FP32, half, or float values.

How to handle the "No node with name ..." error?

The model optimizer can't access the node that doesn't exist. Make sure to specify the correct placeholder, input node name, or output node name.

How to handle the "Module mxnet was not found. Please install mxnet 1.0.0" error?

To ensure that the model optimizer can convert MXNet models, install MXNet 1.0.0 or higher.

How to handle the "The following error happened while loading mxnet model ..." error?

Make sure that the specified path is correct, that the model exists and is not corrupted, and that you have sufficient permissions to work with the model.
How to handle the "... elements of ... were clipped to infinity while converting a blob for node [...] to ..." error?

When you use the --precision=FP16 command line option, the model optimizer converts all of the blobs in the node to the FP16 type. If a value in a blob is out of the range of valid FP16 values, the model optimizer converts the value to positive or negative infinity. Depending on the model, this can produce incorrect inference results or it might not cause any problems. Inspect the number of these elements and the total number of elements in the used blob that is printed out with the name of the node.

How to handle the "... elements of ... were clipped to zero while converting a blob for node [...] to ..." error?

When you use the --precision=FP16 command line option, the model optimizer converts all of the blobs in the node to the FP16 type. If a value in the blob is so close to zero that it can't be represented as a valid FP16 value, the model optimizer converts it to true zero. Depending on the model, this might produce incorrect inference results or it might not cause any problem. Inspect the number of these elements and the total number of elements in the used blob that is printed out with the name of the node.

How to handle the " topology contains no 'input' layers." error?

The prototxt file for your Caffe topology might be intended for training when the model optimizer expects a deploy-ready .prototxt file. To prepare a deploy-ready .prototxt file, follow the instructions provided on GitHub. Typically, preparing a deploy-ready topology involves removing data layers, adding input layers, and removing loss layers.

DeepLens_Kinesis_Video Module for Amazon Kinesis Video Streams Integration

The Amazon Kinesis Video Streams for AWS DeepLens Video library is a Python module that encapsulates the Kinesis Video Streams Producer SDK for AWS DeepLens devices. Use this module to send video feeds from an AWS DeepLens device to Kinesis Video Streams, and to control when to start and stop video streaming from the device. This is useful if you need to train your own deep-learning model. In this case, you can send video feeds of given time intervals from your AWS DeepLens device to Kinesis Video Streams and use the data as an input for the training.

The module, DeepLens_Kinesis_Video, is already installed on your AWS DeepLens device. You can call this module in a Lambda function that is deployed to your AWS DeepLens device as part of a AWS DeepLens project.

The following Python example shows how to use the DeepLens_Kinesis_Video module to stream five-hour video feeds from the caller's AWS DeepLens device to Kinesis Video Streams.

```python
import time
import os
import DeepLens_Kinesis_Video as dkv
from botocore.session import Session
import greengrasssdk

def greengrass_hello_world_run():
    # Create the green grass client so that we can send messages to IoT console
    client = greengrasssdk.client('iot-data')
```

139
iot_topic = '{}\aws/\things/{}/infer'.format(os.environ['AWS_IOT_THING_NAME'])

# Stream configuration, name and retention
# Note that the name will appear as deepLens-myStream
stream_name = 'myStream'
retention = 2 # hours

# Amount of time to stream
wait_time = 60 * 60 * 5 # seconds

# Use the boto session API to grab credentials
session = Session()
creds = session.get_credentials()

# Create producer and stream.
producer = dkv.createProducer(creds.access_key, creds.secret_key, creds.token, "us-east-1")
client.publish(topic=iot_topic, payload="Producer created")
kvs_stream = producer.createStream(stream_name, retention)
client.publish(topic=iot_topic, payload="Stream {} created".format(stream_name))

# Start putting data into the KVS stream
kvs_stream.start()
client.publish(topic=iot_topic, payload="Stream started")
time.sleep(wait_time)
# Stop putting data into the KVS stream
kvs_stream.stop()
client.publish(topic=iot_topic, payload="Stream stopped")

# Execute the function above
greengrass_hello_world_run()

In this example, we call `dkv.createProducer` to instantiate the Kinesis Video Streams Producer SDK client. We then call the `producer.createStream` to set up streaming from the AWS DeepLens device. We control the length of video feeds by calling `my_stream.start`, `time.sleep` and `my_stream.stop`. The stored video is retained in Kinesis Video Streams for two hours because we set the retention parameter to 2.

Topics
- DeepLens_Kinesis_Video.createProducer Function (p. 140)
- Producer Object (p. 141)
- Stream Object (p. 142)

DeepLens_Kinesis_Video.createProducer Function

Creates an instance of the Kinesis Video Streams Producer SDK client object for AWS DeepLens. Use the instance to connect your AWS DeepLens device to the AWS Cloud and to manage video streams from the device to Kinesis Video Streams.

Syntax

```python
import DeepLens_Kinesis_Video as dkv
producer = dkv.createProducer(aws_access_key, aws_secret_key, session_token, aws_region)
```

Parameters
- `aws_access_key`
Type: "string"
Required: Yes
The IAM access key of your AWS account.
• aws_secret_key
Type: "string"
Required: Yes
The IAM secret key of your AWS account.
• session_token
Type: "string"
Required: No
A session token, if any. An empty value means an unspecified token.
• aws_region
Type: "string"
Required: Yes
The AWS Region to stream data to. For AWS DeepLens applications, the only valid value is us-east-1.

Returns
• A Producer object. (p. 141)

Example

```python
import DeepLens_Kinesis_Video as dkv
producer = dkv.createProducer("ABCDEF...LMNO23PU", "abcDEFGHi...bc8defGxhiJ", ",", "us-east-1")
```

**Producer Object**

An object that represents the Kinesis Video Streams Producer SDK client that is used to create streams to which to send video feeds from the AWS DeepLens device.

**Topics**

• Producer.createStream Method (p. 141)

**Producer.createStream Method**

Creates a Kinesis Video Streams stream object to send video feeds from the AWS DeepLens device to.

**Syntax**

```python
stream = producer (p. 141).createStream(stream_name, retention)
```

**Parameters**
• **stream_name**
  
  Type: "string"
  
  Required: Yes
  
  The name of a Kinesis stream that your AWS DeepLens device sends video feeds to. If the stream doesn't exist, Kinesis Video Streams creates it. Otherwise, it uses the existing stream to receive the video feeds. You can have multiple streams as long as they have unique names and handles.

• **retention**
  
  Type: int
  
  Required: Yes
  
  The time, in hours, to retain the streamed data. To view the data in the Stream Preview on the Kinesis Video Streams console, set this parameter to greater than or equal to 2 hours.

**Returns**

• A [Stream](p. 142) object.

---

**Stream Object**

An object that encapsulates a Kinesis stream for video feeds from your AWS DeepLens device and exposes methods for controlling when to start and stop streaming data.

**Topics**

- [Stream.isActive Property](p. 142)
- [Stream.start Method](p. 142)
- [Stream.stop Method](p. 143)

---

**Stream.isActive Property**

Returns a boolean flag to indicate whether the producer is sending data to this stream.

**Syntax**

```
stream (p. 142).isActive
```

**Parameters**

• None

**Returns**

• Type: Boolean
  
  Value: `true` if the stream is active. Otherwise, `false`.

---

**Stream.start Method**

Notifies the producer to start sending video feeds from your AWS DeepLens device to the Kinesis stream.
Stream Object

Syntax

```java
stream (p. 142).start()
```

Parameters

• None

Returns

• None

Stream.stop Method

Notifies the producer to stop sending video feeds from your AWS DeepLens device to the Kinesis stream.

Syntax

```java
stream (p. 142).stop()
```

Parameters

• None

Returns

• None
Security

This section provides guidelines for securing different aspects of AWS DeepLens.

Topics

• Data Protection (p. 144)
• Identity and Access Management for AWS DeepLens (p. 144)
• Update Management (p. 157)
• Security Compliance (p. 157)

Data Protection

AWS DeepLens does not collect data from the device. Video frames from the camera and inference results are confined to the device locally. As a user, you control how and where to publish inference results to other AWS services in the project's Lambda function. Your account remains the sole ownership of the affected data regardless which service it is published to.

The AWS DeepLens supports hardware-level full-disk encryption for the data storage on device. You must configure data encryption on the device.

For the purpose of device registration and maintenance, communications between your AWS DeepLens device and your computer requires HTTPS connection, except for connecting to the device softAP endpoint in the device setup mode that requires authentication with password. The default password is printed at the bottom of the AWS DeepLens device.

For on-device disk encryption, keys are stored in a hardware component known as Trusted Platform Module (TPM).

Models are never deleted from the device. To remove data from the device, you must connect to the AWS DeepLens device using SSH and manually remove data. You can also perform a factory reset.

Identity and Access Management for AWS DeepLens

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use AWS DeepLens resources. IAM is an AWS service that you can use with no additional charge.

Topics

• Audience (p. 145)
• Authenticating With Identities (p. 145)
• Managing Access Using Policies (p. 147)
• How AWS DeepLens Works with IAM (p. 148)
• AWS DeepLens Identity-Based Policy Examples (p. 150)
Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in AWS DeepLens.

Service user – If you use the AWS DeepLens service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more AWS DeepLens features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in AWS DeepLens, see Troubleshooting AWS DeepLens Identity and Access (p. 156).

Service administrator – If you're in charge of AWS DeepLens resources at your company, you probably have full access to AWS DeepLens. It’s your job to determine which AWS DeepLens features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with AWS DeepLens, see How AWS DeepLens Works with IAM (p. 148).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to AWS DeepLens. To view example AWS DeepLens identity-based policies that you can use in IAM, see AWS DeepLens Identity-Based Policy Examples (p. 150).

Authenticating With Identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company’s single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the AWS Sign-In User Guide.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don’t use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the IAM User Guide.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the AWS IAM Identity Center User Guide and Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don’t use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list...
of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the IAM User Guide.

IAM Users and Groups

An IAM user is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the IAM User Guide.

An IAM group is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named IAMAdmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the IAM User Guide.

IAM Roles

An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the IAM User Guide. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the AWS IAM Identity Center User Guide.

- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.

- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.

- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.

- **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, Resources, and Condition Keys for AWS DeepLens in the Service Authorization Reference.
• **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](https://docs.aws.amazon.com/IAM/latest/UserGuide/id服务role.html) in the IAM User Guide.

• **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

• **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_instances.html) in the IAM User Guide.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role (instead of a user)](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_users.html) in the IAM User Guide.

### Managing Access Using Policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_overview.html) in the IAM User Guide.

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

### Identity-Based Policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_creating.html) in the IAM User Guide.

Identity-based policies can be further categorized as inline policies or managed policies. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_changing.html) in the IAM User Guide.

### Resource-Based Policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM role trust policies and Amazon S3 bucket policies. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the
resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can’t use AWS managed policies from IAM in a resource-based policy.

**Access Control Lists (ACLs)**

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the Amazon Simple Storage Service Developer Guide.

**Other Policy Types**

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity’s identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the IAM User Guide.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session’s permissions are the intersection of the user or role’s identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the IAM User Guide.

**Multiple Policy Types**

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the IAM User Guide.

**How AWS DeepLens Works with IAM**

Before you use IAM to manage access to AWS DeepLens, you should understand what IAM features are available to use with AWS DeepLens. To get a high-level view of how AWS DeepLens and other AWS services work with IAM, see AWS Services That Work with IAM in the IAM User Guide.

**Topics**

- AWS DeepLens Identity-Based Policies (p. 149)
AWS DeepLens Identity-Based Policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. AWS DeepLens supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the IAM User Guide.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as permission-only actions that don’t have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called dependent actions.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in AWS DeepLens use the following prefix before the action: aws-deeplens:. For example, to grant someone permission to run an Amazon EC2 instance with the Amazon EC2 RunInstances API operation, you include the ec2:RunInstances action in their policy. Policy statements must include either an Action or NotAction element. AWS DeepLens defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

"Action": [
  "ec2:action1",
  "ec2:action2"
]

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word Describe, include the following action:

"Action": "ec2:Describe*"

To see a list of AWS DeepLens actions, see Actions Defined by AWS DeepLens in the IAM User Guide.

Resources

AWS DeepLens does not support specifying resource ARNs in a policy.

Condition Keys

AWS DeepLens does not provide any service-specific condition keys.

AWS DeepLens Resource-Based Policies

AWS DeepLens does not support resource-based policies.
Access Control Lists (ACLs)

AWS DeepLens does not support access control lists (ACLs).

Authorization Based on AWS DeepLens Tags

AWS DeepLens does not support tagging resources or controlling access based on tags.

AWS DeepLens IAM Roles

An IAM role is an entity within your AWS account that has specific permissions.

Using Temporary Credentials with AWS DeepLens

AWS DeepLens supports using temporary credentials.

Service-Linked Roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

AWS DeepLens does not support service-linked roles.

Service Roles

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

AWS DeepLens supports service roles.

Choosing an IAM Role in AWS DeepLens

When you create a widget resource in AWS DeepLens, you must choose a role to allow AWS DeepLens to access Amazon EC2 on your behalf. If you have previously created a service role or service-linked role, then AWS DeepLens provides you with a list of roles to choose from. It's important to choose a role that allows access to start and stop Amazon EC2 instances. For more information, see ADD XREF TO YOUR DOCS HERE.

AWS DeepLens Identity-Based Policy Examples

By default, IAM users and roles don't have permission to create or modify AWS DeepLens resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating Policies on the JSON Tab in the IAM User Guide.

Topics

- Policy Best Practices (p. 151)
- Using the AWS DeepLens Console (p. 151)
- Allow Users to View Their Own Permissions (p. 156)
Policy Best Practices

Identity-based policies determine whether someone can create, access, or delete AWS DeepLens resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the AWS managed policies that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the IAM User Guide.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as least-privilege permissions. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the IAM User Guide.

- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the IAM User Guide.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the IAM User Guide.

- **Require multi-factor authentication (MFA)** – if you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the IAM User Guide.

For more information about best practices in IAM, see Security best practices in IAM in the IAM User Guide.

Using the AWS DeepLens Console

To access the AWS DeepLens console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS DeepLens resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won’t function as intended for entities (IAM users or roles) with that policy.

To ensure that those entities can still use the AWS DeepLens console, also attach the following AWS managed policy to the entities. For more information, see Adding Permissions to a User in the IAM User Guide:

```json
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "DeepLensIoTThingAccess",
        "Effect": "Allow",
        "Action": [
          "iot:CreateThing",
          "iot:DeleteThing",
          "iot:DeleteThingShadow",
```
```json
{
  "Sid": "DeepLensIoTIdentityAccess",
  "Effect": "Allow",
  "Action": [  
    "iot:GetCurrentAccount",
    "iot:GetSubscriptionArn",
    "iot:GetShadowRoot",
    "iot:GetThing",
    "iot:ListAttachedPrincipalPolicies",
    "iot:ListAttachedThingPolicies",
    "iot:ListCertificates",
    "iot:ListPrincipalPolicies",
    "iot:ListThings",
    "iot:ListThingShadowStates",
    "iot:ListThingTypes"
  ],
  "Resource": [
    "arn:aws:iot:*:*:thing/deeplens_*"
  ]
},
{
  "Sid": "DeepLensIoTCertificateAccess",
  "Effect": "Allow",
  "Action": [  
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal"
  ],
  "Resource": [
    "arn:aws:iot:*:*:thing/deeplens_*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid": "DeepLensIoTCreateCertificateAndPolicyAccess",
  "Effect": "Allow",
  "Action": [  
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [  
    "iot:AttachPrincipalPolicy"
  ],
  "Resource": [
    "arn:aws:iot:*:*:policy/deeplens*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid": "DeepLensIoTDataAccess",
  "Effect": "Allow",
  "Action": [  
    "iot:GetThingShadow",
    "iot:UpdateThingShadow"
  ],
  "Resource": [
    "arn:aws:iot:*:*:thing/deeplens_*"
  ]
},
{
  "Sid": "DeepLensIoTEndpointAccess",
  "Effect": "Allow",
  "Action": [  
    "iot:DescribeEndpoint"
  ],
  "Resource": [
    "*"
  ]
}
```
"Sid": "DeepLensAccess",
"Effect": "Allow",
"Action": [
  "deeplens:*"
],
"Resource": [ 
  "*"
],

},

{"Sid": "DeepLensS3ObjectAccess",
"Effect": "Allow",
"Action": [
  "s3:GetObject"
],
"Resource": [ 
  "arn:aws:s3:::deeplens*/*"
]
},

{"Sid": "DeepLensS3Buckets",
"Effect": "Allow",
"Action": [
  "s3:DeleteBucket",
  "s3:ListBucket"
],
"Resource": [ 
  "arn:aws:s3:::deeplens*"
]
},

{"Sid": "DeepLensCreateS3Buckets",
"Effect": "Allow",
"Action": [
  "s3:CreateBucket"
],
"Resource": [ 
  "*"
]
},

{"Sid": "DeepLensIAMPassRoleAccess",
"Effect": "Allow",
"Action": [
  "iam:PassRole"
],
"Resource": [ 
  "*"
],
"Condition": {
  "StringEquals": {
    "iam:PassedToService": [ 
      "greengrass.amazonaws.com",
      "sagemaker.amazonaws.com"
    ]
  }
}
},

{"Sid": "DeepLensIAMLambdaPassRoleAccess",
"Effect": "Allow",
"Action": [
  "iam:PassRole"
],
"Resource": [ 
  "arn:aws:iam::*:role/deeplens*"
]
],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      }
    }
  },
  {
    "Sid": "DeepLensGreenGrassAccess",
    "Effect": "Allow",
    "Action": [
      "greengrass:AssociateRoleToGroup",
      "greengrass:AssociateServiceRoleToAccount",
      "greengrass:CreateResourceDefinition",
      "greengrass:CreateResourceDefinitionVersion",
      "greengrass:CreateCoreDefinition",
      "greengrass:CreateCoreDefinitionVersion",
      "greengrass:CreateDeployment",
      "greengrass:CreateFunctionDefinition",
      "greengrass:CreateFunctionDefinitionVersion",
      "greengrass:CreateGroup",
      "greengrass:CreateGroupCertificateAuthority",
      "greengrass:CreateGroupVersion",
      "greengrass:CreateLoggerDefinition",
      "greengrass:CreateLoggerDefinitionVersion",
      "greengrass:CreateSubscriptionDefinition",
      "greengrass:CreateSubscriptionDefinitionVersion",
      "greengrass:DeleteCoreDefinition",
      "greengrass:DeleteFunctionDefinition",
      "greengrass:DeleteGroup",
      "greengrass:DeleteLoggerDefinition",
      "greengrass:DeleteSubscriptionDefinition",
      "greengrass:DisassociateRoleFromGroup",
      "greengrass:DisassociateServiceRoleFromAccount",
      "greengrass:GetAssociatedRole",
      "greengrass:GetConnectivityInfo",
      "greengrass:GetCoreDefinition",
      "greengrass:GetCoreDefinitionVersion",
      "greengrass:GetDeploymentStatus",
      "greengrass:GetDeviceDefinition",
      "greengrass:GetDeviceDefinitionVersion",
      "greengrass:GetFunctionDefinition",
      "greengrass:GetFunctionDefinitionVersion",
      "greengrass:GetGroup",
      "greengrass:GetGroupCertificateAuthority",
      "greengrass:GetGroupCertificateConfiguration",
      "greengrass:GetGroupVersion",
      "greengrass:GetLoggerDefinition",
      "greengrass:GetLoggerDefinitionVersion",
      "greengrass:GetServiceRoleForAccount",
      "greengrass:GetSubscriptionDefinition",
      "greengrass:GetSubscriptionDefinitionVersion",
      "greengrass:ListGroupCertificateAuthorities",
      "greengrass:ListGroupDefinitions",
      "greengrass:ListGroupVersions",
      "greengrass:ListGroupGroups",
      "greengrass:ListGroupSubscriptionDefinitionVersions",
      "greengrass:ListGroupSubscriptionDefinitions",
      "greengrass:ListDeployments",
      "greengrass:ListDeviceDefinitionVersions",
      "greengrass:ListDeviceDefinitions",
      "greengrass:ListFunctionDefinitionVersions",
      "greengrass:ListFunctionDefinitions",
      "greengrass:ListGroupCertificateAuthorities",
      "greengrass:ListGroupDefinitions",
      "greengrass:ListGroupVersions",
      "greengrass:ListGroups",
      "greengrass:ListLoggerDefinitionVersions",
      "greengrass:ListLoggerDefinitions",
      "greengrass:ListSubscriptionDefinitionVersions",
      "greengrass:ListSubscriptionDefinitions"}
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
"greengrass:UpdateFunctionDefinition",
"greengrass:UpdateGroup",
"greengrass:UpdateGroupCertificateConfiguration",
"greengrass:UpdateLoggerDefinition",
"greengrass:UpdateSubscriptionDefinition"
],
"Resource": [ "*"

},
{
"Sid": "DeepLensLambdaAdminFunctionAccess",
"Effect": "Allow",
"Action": [ "lambda:CreateFunction",
"lambda:DeleteFunction",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:ListFunctions",
"lambda:ListVersionsByFunction",
"lambda:PublishVersion",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration"
],
"Resource": [ 
"arn:aws:lambda:*:*:function:deeplens*"

},
{
"Sid": "DeepLensSageMakerAccess",
"Effect": "Allow",
"Action": [ 
"sagemaker:CreateTrainingJob",
"sagemaker:DescribeTrainingJob",
"sagemaker:StopTrainingJob"
],
"Resource": [ 
"arn:aws:sagemaker:*:*:training-job/deeplens_*"

},
{
"Sid": "DeepLensAcuityStreamAccess",
"Effect": "Allow",
"Action": [ 
"acuity:CreateStream",
"acuity:DescribeStream",
"acuity:DeleteStream"
]
"Resource": [ 
"arn:aws:acuity:*:*:stream/deeplens/*"

},
{
"Sid": "DeepLensAcuityEndpointAccess",
"Effect": "Allow",
"Action": [ 
"acuity:GetDataEndpoint"
],
"Resource": [ 
"*"

}
More granular access is not encouraged. The device is typically accessed through the console and not through API calls. There are no public APIs for AWS DeepLens.

Allow Users to View Their Own Permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"],
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*
    }
  ]
}
```

Troubleshooting AWS DeepLens Identity and Access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS DeepLens and IAM.

Topics
- I Am Not Authorized to Perform an Action in AWS DeepLens (p. 156)
- I Am Not Authorized to Perform iam:PassRole (p. 157)

I Am Not Authorized to Perform an Action in AWS DeepLens

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.
The following example error occurs when the mateojackson IAM user tries to use the console to view details about a fictional my-example-widget resource but doesn't have the fictional DeepLens:GetWidget permissions.

User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: DeepLens:GetWidget on resource: my-example-widget

In this case, the policy for the mateojackson user must be updated to allow access to the my-example-widget resource by using the DeepLens:GetWidget action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I Am Not Authorized to Perform iam:PassRole

If you receive an error that you're not authorized to perform the iam:PassRole action, your policies must be updated to allow you to pass a role to AWS DeepLens.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named marymajor tries to use the console to perform an action in AWS DeepLens. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

In this case, Mary's policies must be updated to allow her to perform the iam:PassRole action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

Update Management

AWS DeepLens makes available device software updates. As a user, you decide whether or not to install the updates to the device. You can do so in the AWS DeepLens console. For a security patch, you'll be forced to install the patch.

AWS DeepLens provides device software updates, periodically, as software patches or new features. You can choose to re-flash the image.

Security Compliance

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:
• **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.

• **Architecting for HIPAA Security and Compliance on Amazon Web Services** – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

  **Note**

  Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

• **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.

• **Evaluating Resources with Rules** in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.

• **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).

• **AWS Audit Manager** – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.
AWS DeepLens End of Life

Starting January 31, 2024, you can no longer access AWS DeepLens through the AWS management console, manage AWS DeepLens devices, or access any projects you have created.

AWS DeepLens end of life FAQ

Use the following sections to get answers to commonly asked questions about the AWS DeepLens end of life.

Q. What happens to my AWS DeepLens resources after the end of life (EOL) date?

After January 31, 2024, all references to AWS DeepLens models, projects, and device information are deleted from the AWS DeepLens service. You can no longer discover or access the AWS DeepLens service from your AWS console and applications that call the AWS DeepLens API no longer work.

Q. Will I be billed for AWS DeepLens resources remaining in my account after the EOL date?

Resources created by AWS DeepLens, such as Amazon S3 buckets, AWS Lambda functions, AWS IoT things, and AWS Identity and Access Management (IAM) roles continue to exist on their respective services after January 31, 2024. To avoid being billed after AWS DeepLens is no longer supported, follow all of these steps (p. 162) to delete these resources.

Q. How do I delete my AWS DeepLens resources?

To delete the resources used by AWS DeepLens and learn how to restore your AWS DeepLens device to factory settings, see the section called “Delete your AWS DeepLens device resources”.

Q. Can I deploy my AWS DeepLens projects after the end of life (EOL) date?

You can deploy AWS DeepLens projects until January 31, 2024. After that date, you do not have access to the AWS DeepLens console or API and any application that calls on the AWS DeepLens API does not work.

Q. Will my AWS DeepLens device continue to receive security updates?

AWS DeepLens is not updated after January 31, 2024. While some applications deployed on AWS DeepLens devices might continue to run after the EOL date, AWS does not provide remedies related to and is not responsible for any issue arising from AWS DeepLens software or hardware.

Q. How can I continue to get hands-on experience with AWS AI/ML?

We suggest you try our other hands-on machine learning tools. With AWS DeepRacer, use a cloud-based 3D racing simulator to create reinforcement learning models for an autonomous 1/18th scale race car.
Learn and experiment in a no-setup, free development environment with Amazon SageMaker Studio Lab. Automate your image and video analysis with Amazon Rekognition, or use AWS Panorama to improve your operations with computer vision at the edge.

**Q. What should I do with my AWS DeepLens device?**

We encourage you to recycle your AWS DeepLens device through the Amazon Recycling Program. Amazon covers the costs associated with shipping and recycling.

**Delete your AWS DeepLens device resources**

The following sections guide you through the process of exporting your models from the AWS DeepLens device via Secure Shell (SSH) protocol, deleting the remaining cloud resources used by AWS DeepLens, and how to restore your AWS DeepLens device to factory settings.

- **Access your AWS DeepLens device via SSH terminal** (p. 160)
- **Retrieve model artifacts from the AWS DeepLens device** (p. 160)
- **Delete model artifacts from your AWS DeepLens device** (p. 161)
- **Delete user logs from your AWS DeepLens device** (p. 161)
- **Delete Lambda functions deployed through AWS IoT Greengrass** (p. 161)
- **Delete model artifacts from your AWS DeepLens device** (p. 161)

**Access your AWS DeepLens device via SSH terminal**

Before you can access your device using an SSH terminal, you must turn on your AWS DeepLens device's SSH server. This process is different for each version of the AWS DeepLens hardware. The hardware version is printed on the bottom of the device. Version 1.1 of the AWS DeepLens device has V1.1 marked on the bottom of the device. If your device does not have V1.1 marked, it is an AWS DeepLens V1.

- To check the status of the SSH server on the AWS DeepLens device V1, see [Set Up Your AWS DeepLens Device](p. 27).
- To check the status of the SSH server on the AWS DeepLens device V1.1, see [View or Update Your AWS DeepLens 2019 Edition (v1.1) Device Settings](p. 19).

Once you confirm that your AWS DeepLens device SSH server is on, you need the device's IP address to start an SSH session. To obtain your AWS DeepLens device's IP address via the AWS DeepLens console, do the following:

1. Log in to your AWS console and navigate to [AWS DeepLens](p. 160).
2. Choose [Devices](p. 160) from the main navigation pane.
3. From the device list, choose your AWS DeepLens device to open the device information page.
4. From the [Device details](p. 160) section, copy a local IP address of the selected AWS DeepLens device.

**Retrieve model artifacts from the AWS DeepLens device**

1. Connect the AWS DeepLens device to a computer using a USB cable.
2. Make sure the AWS DeepLens device and your computer are on the same network.
3. Start a terminal and enter the following SSH command, replacing `your_device_ip` with the IP address you copied from the [Access your AWS DeepLens device via SSH terminal](p. 160) section:
Delete your AWS DeepLens device resources

4. Use the following command to navigate to the artifacts folder and list its contents:

```bash
cd /opt/awscam/artifacts && ls
```

5. Exit the SSH session.

6. To copy the artifacts folder from your AWS DeepLens device to your computer, start a terminal and enter the following command:

```bash
scp -r aws_cam@your_device_ip:/opt/awscam/artifacts/ ./artifacts/
```

7. When prompted, enter the AWS DeepLens device password.

8. Wait for the copy operation to finish.

Delete model artifacts from your AWS DeepLens device

1. Start a terminal and enter the following SSH command:

```bash
ssh aws_cam@your_device_ip
```

2. Log in as the root user by entering the following command:

```bash
sudo su
```

3. When prompted, enter the AWS DeepLens device password.

4. Delete the model artifacts by entering the following command:

```bash
rm /opt/awscam/artifacts/*
```

Delete user logs from your AWS DeepLens device

1. Start a terminal and enter the following SSH command:

```bash
ssh aws_cam@your_device_ip
```

2. Log in as the root user by entering the following command:

```bash
sudo su
```

3. When prompted, enter the AWS DeepLens device password.

4. Delete the user logs by entering the following command:

```bash
rm -r /opt/awscam/greengrass/ggc/var/log/user
```

Delete Lambda functions deployed through AWS IoT Greengrass

1. Start a terminal and enter the following SSH command:

```bash
ssh aws_cam@your_device_ip
```
Delete your AWS DeepLens cloud resources

When you register your device and use the AWS DeepLens console, the service creates multiple resources on your AWS account in addition to AWS DeepLens models, projects, and devices. These resources include Amazon S3 buckets, AWS Lambda functions, AWS IoT things, and IAM roles.

The following sections guide you through the process of deleting all remaining AWS DeepLens cloud resources.

- Delete model entries from the AWS DeepLens console  (p. 162)
- Delete projects from the AWS DeepLens console  (p. 162)
- Deregister AWS DeepLens devices  (p. 162)
- Delete AWS DeepLens S3 buckets  (p. 163)
- Delete AWS DeepLens IoT resources  (p. 163)
- Delete AWS DeepLens Lambda functions  (p. 163)
- Delete AWS DeepLens IAM roles  (p. 163)

Delete model entries from the AWS DeepLens console

2. In the navigation pane, choose Models.
3. Select the model you want to delete, then choose Delete.
4. Repeat step 3 for every model entry you want to delete.

Delete projects from the AWS DeepLens console

2. In the navigation pane, choose Projects.
3. Select the project you want to delete.
4. For Actions, choose Delete.
5. Repeat step 3 and step 4 for every project you want to delete.

Deregister AWS DeepLens devices

2. In the navigation pane, choose Devices, then select the device that you want to deregister.
3. Next to the Current project on the selected device page, choose Remove current project from device.
4. When prompted, choose Yes to confirm.
5. Next to Device Settings, choose Deregister.
6. When prompted, choose Deregister to confirm.
7. Your AWS DeepLens is now deregistered. Repeat each of these steps for every AWS DeepLens device on your Devices list.

Delete AWS DeepLens S3 buckets

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Buckets list search bar, enter deeplens-* to only show AWS DeepLens S3 buckets.
3. Select the option next to the name of the bucket that you want to delete, and then choose Delete at the top of the page.
   
   Note
   If the bucket contains any objects, empty the bucket before deleting it by selecting the empty bucket configuration link in the This bucket is not empty error alert and following the instructions on the Empty bucket page. Then return to the Delete bucket page and delete the bucket.

Delete AWS DeepLens IoT resources

1. Sign in to the AWS Management Console and open the AWS IoT console at https://console.aws.amazon.com/iot/.
2. To delete AWS IoT things:
   a. In the navigation pane, choose Manage.
   b. From All Devices, select Things.
   c. In the Things list search bar, enter deeplens to only show AWS DeepLens Things.
   d. Select the checkboxes of all AWS IoT things you want to delete, and then choose Delete at the top of the page.
3. To delete AWS IoT Greengrass resources:
   a. Sign in to the AWS Management Console and open the AWS IoT console at https://console.aws.amazon.com/iot/.
   b. In the navigation pane, choose Manage.
   c. From Greengrass devices, select Groups (V1).
   d. In the Greengrass groups list search bar, enter deeplens to only show AWS DeepLens groups.
   e. Select the check boxes next to the AWS IoT Greengrass groups that you want to delete, and then choose Delete at the top of the page.

Delete AWS DeepLens Lambda functions

1. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/.
2. In the navigation pane, choose Functions.
3. In the Functions list search bar, enter deeplens to only show AWS DeepLens Lambda functions.
4. Select the check boxes next to the Lambda functions that you want to delete, and then choose Delete at the top of the page.

Delete AWS DeepLens IAM roles

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/
2. In the navigation pane, choose Roles.
3. In the Roles list search bar, enter `deeplens` to show a filtered list of AWS DeepLens roles.
4. Select the checkboxes next to the role names that you want to delete, and then choose **Delete** at the top of the page.

**AWS DeepLens device troubleshooting**

See these additional resources if you encounter any issues with your device:

- [Troubleshooting AWS DeepLens (p. 109)]
- [AWS DeepLens forum.]
- [AWS DeepLens FAQs]

If you need additional support reach out to [awsdeeplens@amazon.com].
# Document History for AWS DeepLens

- **API version**: 2017-08-31

The following table describes the additions and changes to the AWS DeepLens Developer Guide documentation.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Bird Classification Sample Project (p. 165)</strong></td>
<td>Adds Bird Classification to the AWS DeepLens Sample Projects. For more information see The Bird Classification Sample Project.</td>
<td>April 8, 2019</td>
</tr>
<tr>
<td><strong>Support for models created with TensorFlow and Caffe (p. 165)</strong></td>
<td>Adds TensorFlow and Caffe as supported modeling frameworks. For more information see Supported TensorFlow Models and Layers and Supported Caffe Models and Layers.</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td><strong>Simplified IAM roles creation (p. 165)</strong></td>
<td>Enables creation of required IAM roles to run your AWS DeepLens app project with a single click of a button in the AWS DeepLens console. For more information, see Register Your Device.</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td><strong>Secure boot (p. 165)</strong></td>
<td>Adds secure booting. The AWS DeepLens device securely boots to prevent the installation of unauthorized operating systems. For more information see Securely Boot Your Device.</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td><strong>Integration with Amazon Kinesis Video Streams (p. 165)</strong></td>
<td>Uses the Kinesis Video Streams for AWS DeepLens Video library to send video feeds from an AWS DeepLens device to Kinesis Video Streams for a specified</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Ability to view device output streams in a browser (p. 165)</td>
<td>Adds support for using a browser to view unprocessed device streams or processed project streams. For more information, see View Your AWS DeepLens Device Output in a Browser.</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td>Named device setup URL (p. 165)</td>
<td>Makes the AWS DeepLens device setup app accessible through the URL of <a href="http://deeplens.config">http://deeplens.config</a>. For more information see Set up Your Device.</td>
<td>June 5, 2018</td>
</tr>
<tr>
<td>Troubleshooting Guide (p. 165)</td>
<td>Provides a list of commonly asked questions and answers about troubleshooting common AWS DeepLens issues. For more information see Troubleshooting Guide.</td>
<td>May 3, 2018</td>
</tr>
<tr>
<td>Gluon support (p. 165)</td>
<td>Adds support for Gluon. For more information, see Supported MXNet Models Exposed by the Gluon API.</td>
<td>March 13, 2018</td>
</tr>
<tr>
<td>Importing from SageMaker (p. 165)</td>
<td>Simplifies the process for importing a model trained with SageMaker. For more information, see Importing Your SageMaker-Trained Model.</td>
<td>February 22, 2018</td>
</tr>
<tr>
<td>Model optimization (p. 165)</td>
<td>Adds support for optimizing your custom model so that it runs on the GPU instead of the CPU. For more information, see Optimize a Custom Model and Model Optimization (mo) Module.</td>
<td>January 31, 2018</td>
</tr>
<tr>
<td>AWS DeepLens Developer Guide (p. 165)</td>
<td>The first release of the programmer's guide to building edge-optimized computer vision applications using AWS DeepLens with inference models trained in common deep learning frameworks, including MXNet.</td>
<td>November 29, 2017</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS Glossary Reference.