

Creating an AWS Root Access Key

Background:

To successfully use Amazon S3 with eStore or Lightbox Ultimate, you need an Amazon Web Services (AWS) “**Access Key**.” The Access Key allows others to programmatically access the contents of your S3 buckets in a secure manner. There are two kinds of Access Keys; “**Root**” and “**User**.” For eStore and Lightbox Ultimate, you need to use your **Root Access Key**.

Access Keys consist of two parts; a 20 character public “**Access Key ID**” and a 40 character private “**Secret Access Key**.” The public Access Key ID is used to publicly identify your AWS account; and can be freely distributed. The private Secret Access Key is used by eStore and Lightbox Ultimate to digitally sign API requests; and must be kept secret.

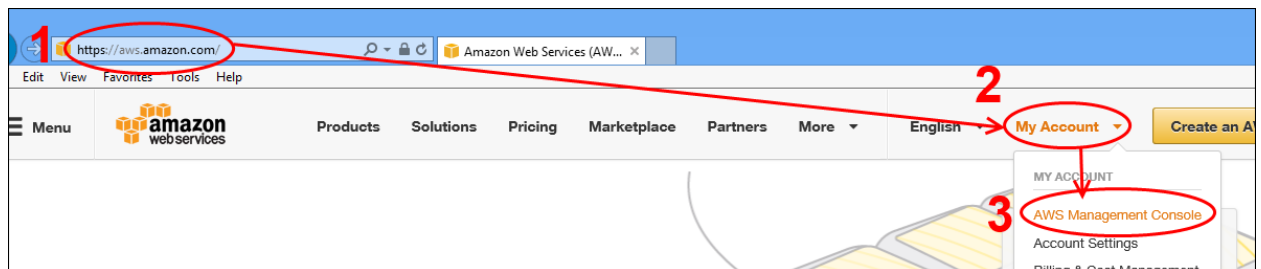
Because the Access Key ID is “public,” do not be alarmed if you ever see it as part of a URL query string in your browser’s address bar. However, if a Secret Access Key becomes known, it is possible for someone to not only access and modify the contents of your S3 buckets; but to do so in a manner that will incur monetary charges against your AWS account.

Until recently, Amazon allowed you to freely lookup the values of both the Access Key ID and Secret Access Key, anytime you wanted. Unfortunately this created a vulnerability; allowing somebody to hack your AWS account and then surreptitiously retrieve your Secret Access Key. Now, because of this; **whenever Access Keys are created, the Secret Access Key will only be shown to you once. If you forget to write down the Secret Access Key, you must create a new Access Key.**

Procedure:

To create a Root Access Key, you must follow this procedure:

1. Goto the AWS home page at: <https://aws.amazon.com> and indicate that you want to sign into the **AWS Management Console**.



2. Now sign into your **AWS account**. You may use your existing Amazon.com email address and password, or create a (new and) separate AWS account. For security reasons, it is recommended that you use an account that is different than your normal Amazon.com account.

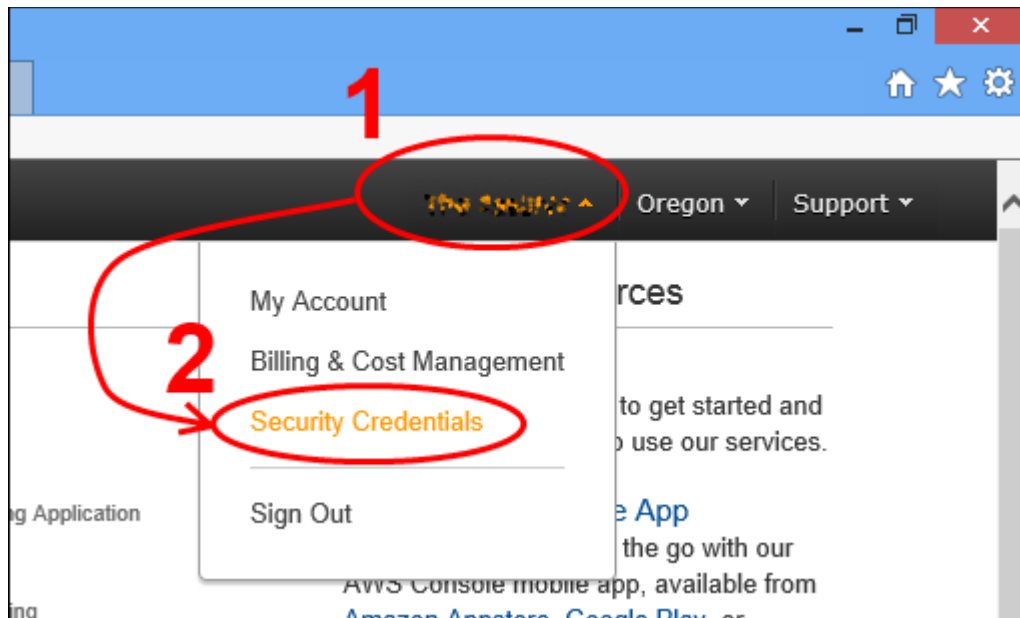
The screenshot shows the Amazon Web Services sign-in page. At the top, the browser address bar displays the URL `https://www.amazon.com/ap/signin?openid.assoc...` and the page title is "Amazon Web Services Sign In". The Amazon Web Services logo is centered at the top of the page. Below the logo, the heading "Sign In or Create an AWS Account" is displayed in orange. A sub-heading states: "You may sign in using your existing Amazon.com account or you can create a new account by selecting 'I am a new user.'".

The form contains the following elements:

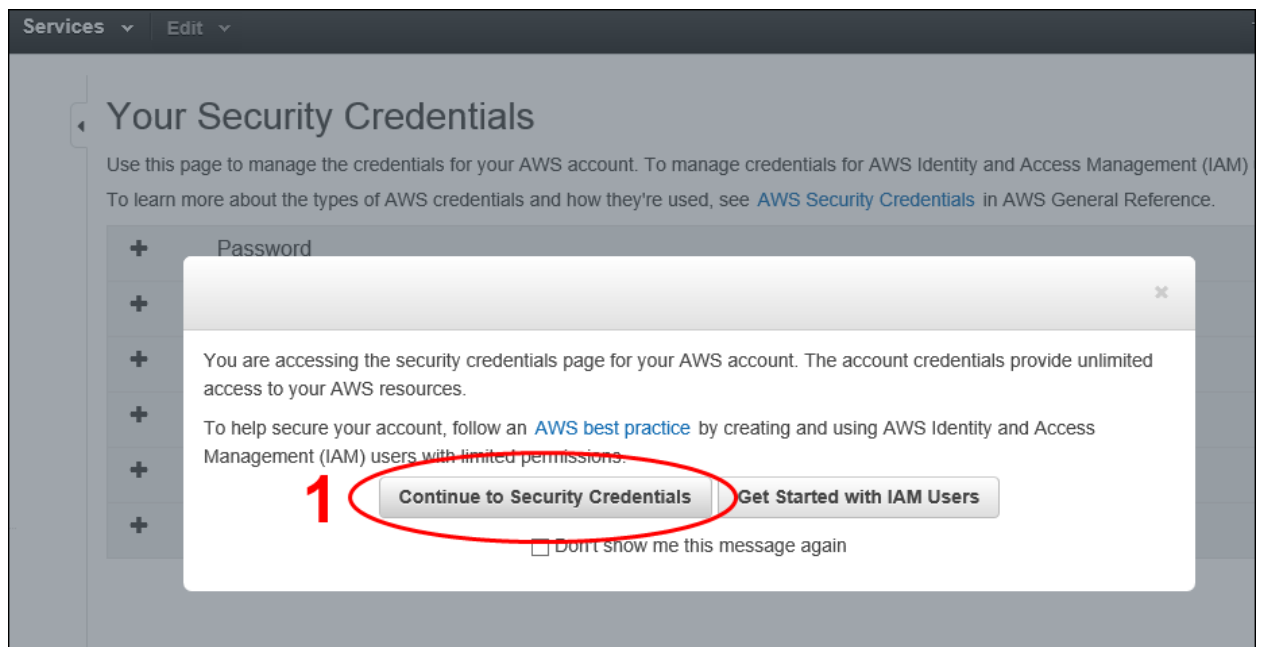
- My e-mail address is:** A text input field containing a partially visible email address. A red circle labeled "1" highlights this field.
- I am a new user.** A radio button option.
- I am a returning user and my password is:** A radio button option that is selected.
- Password field:** A text input field with masked characters (dots). A red circle labeled "2" highlights this field.
- Sign in button:** A yellow button with the text "Sign in using our secure server" and a play icon. A red circle labeled "3" highlights this button.

Below the sign-in button, there are two links: [Forgot your password?](#) and [Has your e-mail address changed?](#)

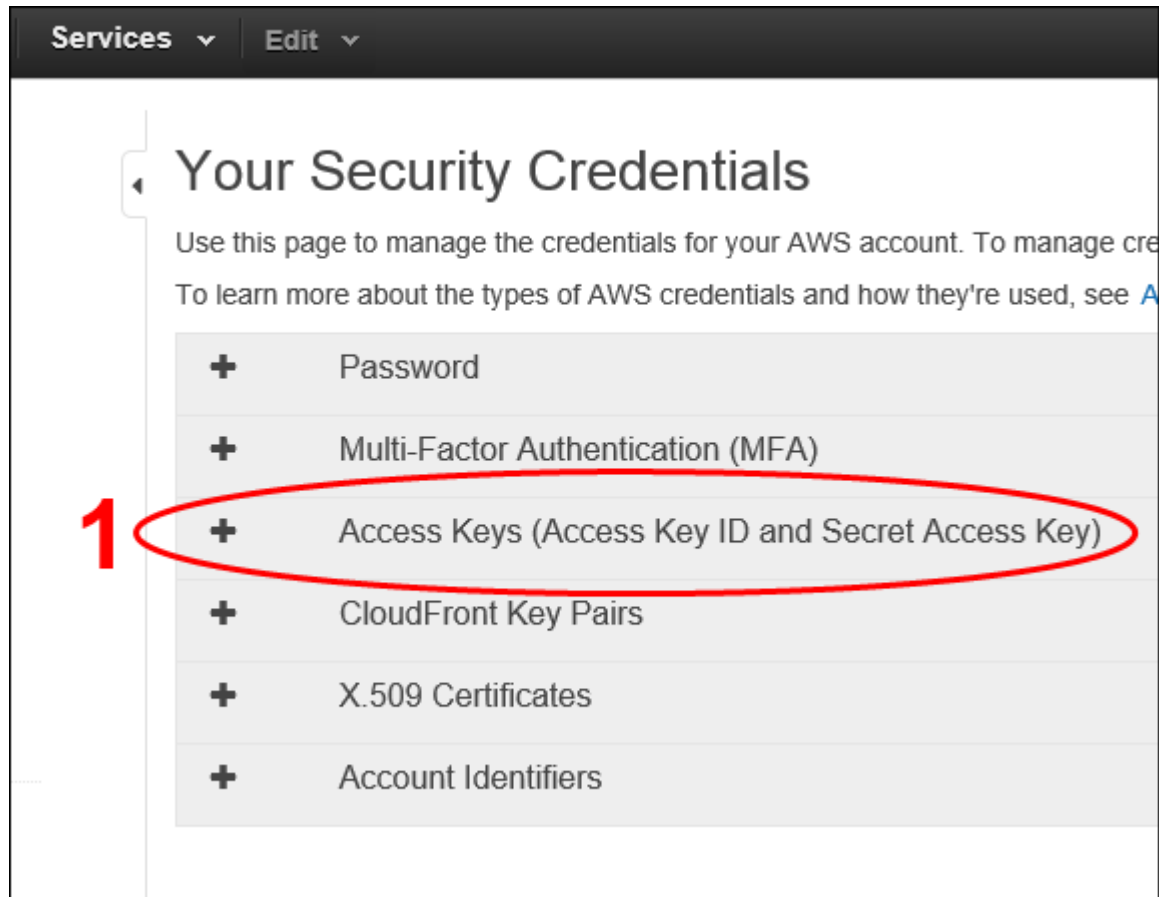
- When the management console appears, indicate that you want to manage your **Security Credentials**.



- If a popup warning appears, click the **“Continue to Security Credentials”** button.



5. An expandable list of available types of AWS security credentials will appear. Indicate that you want to manage your (Root) Access Keys.



6. Access Keys can either be **Active**, **Inactive**, or **Deleted**. An AWS account can have no more than two (2) active or inactive Root Access Keys. If there are more than 2 active or inactive (Root) Access Keys, you will not be allowed to create any new ones; until you first delete an active or inactive Access Key. To create a new (Root) Access Key, click the “**Create New Access Key**” button.

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Status	Actions
1/10/2019	1/10/2019	AKIAI7KXU1D44N17JFAA	Deleted	
1/10/2019	1/10/2019	AKIAI7KXU1D44N17JFAA	Deleted	

2 Create New Access Key

1 Status Deleted Deleted

If you do then this button will not work!

You cannot have more than two (2) Active or Inactive (Root) Access Keys.

Important Change - Managing Your AWS Secret Access Keys
As described in a [previous announcement](#), you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a [best practice](#), we recommend [creating an IAM user](#) that has access keys rather than relying on root access keys.

7. A popup will appear, telling you that your (Root) Access Key was successfully created. To see your Access Key ID and Secret Access Key, click the “**Show Access Key**” link.

Access Keys (Access Key ID and Secret Access Key)

Create Access Key

✓ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

1 Show Access Key

Download Key File Close

Important Change - Managing Your AWS Secret Access Keys

8. The Access Key ID and Secret Access Key will now be visible. **This is the ONLY CHANCE you will have to WRITE DOWN the Secret Access Key.** You also have the opportunity to **DOWNLOAD the newly created (Root) Access Key to your computer, as a CSV file.**

