















# How to login to AWS with Single Sign On

## Table of contents

- 1 [Summary & Scope](#)
- 2 [How to login to AWS with Single Sign On](#)
  - 2.1 [Accessing AWS over the web](#)
  - 2.2 [Accessing AWS on the command line](#)
    - 2.2.1 [Installing maws](#)
    - 2.2.2 [Running maws](#)

Status	<b>READY</b>
Author(s)	Enterprise Information Security Team
Reviewer(s)	<input checked="" type="checkbox"/> Gene Wood <input type="checkbox"/> April King
Classification	<b>MOZILLA CONFIDENTIAL - STAFF AND NDA'D MOZILLIANS ONLY</b>

## Revisions

Version	Published	Changed By	Comment
<b>CURRENT (v. 22)</b>	<b>May 14, 2020 14:08</b>	 <a href="#">April King</a>	Minor tweaks for legibility
v. 21	Apr 14, 2020 13:05	 <a href="#">Gene Wood</a>	
v. 20	Mar 30, 2020 13:59	 <a href="#">Gene Wood</a>	
v. 19	Mar 30, 2020 13:53	 <a href="#">Gene Wood</a>	
v. 18	Dec 11, 2019 09:55	 <a href="#">Gene Wood</a>	
v. 17	Dec 10, 2019 13:29	 <a href="#">Gene Wood</a>	
v. 16	Dec 10, 2019 13:17	 <a href="#">Gene Wood</a>	
v. 15	Nov 26, 2019 17:11	 <a href="#">Gene Wood</a>	
v. 14	Nov 26, 2019 16:34	 <a href="#">Gene Wood</a>	
v. 13	Nov 26, 2019 16:34	 <a href="#">Gene Wood</a>	
v. 12	Nov 26, 2019 16:33	 <a href="#">Gene Wood</a>	
v. 11	Nov 26, 2019 13:06	 <a href="#">Gene Wood</a>	
v. 10	Nov 26, 2019 12:37	 <a href="#">Gene Wood</a>	
v. 9	Nov 26, 2019 11:17	 <a href="#">April King</a>	note about \$(maws)
v. 8	Nov 22, 2019 09:18	 <a href="#">Gene Wood</a>	
v. 7	Nov 22, 2019 09:16	 <a href="#">Gene Wood</a>	
v. 6	Nov 22, 2019 09:11	 <a href="#">Gene Wood</a>	
v. 5	Nov 22, 2019 09:03	 <a href="#">Gene Wood</a>	
v. 4	Nov 22, 2019 09:02	 <a href="#">Gene Wood</a>	
v. 3	Nov 22, 2019 09:01	 <a href="#">Gene Wood</a>	
v. 2	Nov 22, 2019 09:01	 <a href="#">Gene Wood</a>	
v. 1	Nov 22, 2019 08:55	 <a href="#">Gene Wood</a>	

# Summary & Scope

This document describes how an AWS user can access AWS using their federated single sign on login

For instructions on how an AWS account owner can enable federated AWS login with Single Sign On (SSO) in their AWS account visit the [AWS Federated Login Account Setup](#) page

For advanced instructions and details visit the [AWS Federated Login Advanced Details](#) page

## How to login to AWS with Single Sign On

Once the AWS account owner/administrator has [created the identity provider and created some IAM roles](#), users can begin to use single sign on to access AWS either over the web or through the use of the `maws` command line tool.

### Accessing AWS over the web

Browse to <https://aws.sso.mozilla.com/>

Select the role you'd like to assume and you'll be redirected on to AWS.

After 1 to 12 hours when your AWS session expires, AWS will offer you a link to return to [aws.sso.mozilla.com](https://aws.sso.mozilla.com) and refresh your session. Just click the link and you'll get a refreshed session and be sent back to the page on AWS you were on.

If you would like to access AWS over the web as well as on the command line, read below about `maws` and the `-w` option

To learn more about what controls the length of the session, visit this [Advanced Section](#).

### Accessing AWS on the command line

#### Installing maws

The Mozilla AWS CLI (`maws`) is a python command line tool that will allow you to access AWS on the command line with your Mozilla SSO identity. It can be installed using `pip`. We've packaged an additional package that both installs and configures the Mozilla AWS CLI specifically for Mozilla's use.

1. Ensure that you have both [python](#) and [pip](#) installed on your workstation
2. Install `maws` by running `pip install mozilla-aws-cli-mozilla --user --upgrade`



This installs the `mozilla-aws-cli-mozilla` package which has the Mozilla specific SSO configuration as well as the `mozilla-aws-cli` tool which is not specific to Mozilla's use.



If you see the warning `The script maws is installed in '$HOME/.local/bin' which is not on PATH. Consider adding $HOME/.local/bin to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.` you will need to modify your PATH to include that directory. This may also happen for the path `~/Library/Python/<version>/bin` on Mac. You can modify your path on Mac in `/etc/paths` or on Linux `/etc/profile` or `~/.profile`

If you'd like to configure `maws` manually see the [Advanced section](#)

#### Running maws

To run `maws` run it within an evaluated subshell. This can be done a few different ways. Here are some examples of how you could run it

```
$(maws)
eval $(maws)
source <(maws)
```



Using the `$(maws)` subshell syntax with `zsh` and `YADR` causes the IAM role picker to come up a second time unnecessarily. Use one of the other two forms instead: `eval $(maws)` or `source <(maws)`



If you use Firefox Multi-Account Containers and have dedicated container for Mozilla stuff, [check out these instructions](#) on how to get this to work with Mozilla AWS CLI



If you run Python on MacOS Catalina 10.15 and used `brew` to install Python, you may encounter an `openssl` issue which crashes Python with an error about `/usr/lib/libcrypto.dylib` you may need to install `openssl` and add an export to your `.zshrc` file as described here : <https://stackoverflow.com/a/58445755/168874>

In each of these examples if you also wanted `maws` to launch an AWS web console tab in your browser you could add a `-w` so the command would look like `$(maws -w)`

When you start the `maws` tool, it will open a webpage where you can select a role from among your choices. Once you do that, it will either send you back into your terminal or it will redirect you into the AWS web console. The role selector will look like this:

# Mozilla AWS CLI

Please select a role:

## infosec-dev

- [MAWS-Admin](#)
- [MAWS-ReadOnly](#)
- [MAWS-ViewOnly](#)

`maws` has four different modes in which it can operate:

- outputting environmental variables (such as `AWS_SECRET_ACCESS_KEY`) directly (default behavior)
- storing its credentials in a separate credentials file (`-o shared`)
- storing its credentials in the default `awscli` / AWS SDK / `boto3` file (`-o awscli`)
- outputting JSON to be directly consumed by `boto3` or `aws-sdk`

Each of which (aside from the last one) outputs environment variables that you'll want to load into your environment

### Running maws with environmental variable output (the default)

```
$ eval $(maws)
Environment variables set for role arn:aws:iam::123456789012:role/MAWS-Admin
```

### Running maws with a separate credentials file

```
$ $(maws -o shared)
Environment variables set for role arn:aws:iam::123456789012:role/MAWS-Admin

$ cat ~/.config/maws/credentials
[infosec-dev-MAWS-Admin]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token = AQoDYXdzEJr...<remainder of security token>
```

## Running maws with AWS CLI automatic configuration

```
$ source <(maws -o awscli)
Environment variables set for role arn:aws:iam::123456789012:role/MAWS-Admin

$ cat ~/.aws/credentials
[infosec-dev-MAWS-Admin]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
aws_session_token = AQoDYXdzEJr...<remainder of security token>
```

## Automatically logging into the AWS web console

`maws` has the ability to automatically send you into the AWS web interface once you select a role. Simply add `-w` to your command line, and you will be automatically redirected. This can be especially useful in combination with the `-r` flag, which lets you specify a role ARN on the command line.

```
$ alias eis-mawsadmin="eval $(maws -r 'arn:aws:iam::123456789012:role/MAWS-Admin' -w)"
$ eis-mawsadmin
```