





















AWS Federated Login Account Setup

Table of contents

- 1 Summary & Scope
- 2 AWS Federated Login Account Setup
 - 2.1 Step 1 of 4 : Deploy the AWS IAM OIDC Identity Provider in the web UI
 - 2.2 Step 2 of 4 : Determine which user groups to grant access to
 - 2.3 Step 3 of 4 : Create an IAM Role
 - 2.4 Test your new setup
 - 2.5 Step 4 of 4 : Disabling and deleting user roles

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

Revisions

Version	Published	Changed By	Comment
CURRENT (v. 19)	Jun 01, 2020 12:47	 April King  Gene Wood	
v. 18	May 14, 2020 14:58	 April King	Added step 4 of 4 (disabling users)
v. 17	May 14, 2020 09:10	 Gene Wood	
v. 16	Apr 30, 2020 11:18	 Gene Wood	
v. 15	Apr 30, 2020 10:08	 Gene Wood	
v. 14	Mar 18, 2020 12:44	 Gene Wood	
v. 13	Mar 18, 2020 12:44	 Gene Wood	
v. 12	Mar 18, 2020 12:44	 Gene Wood	
v. 11	Dec 30, 2019 17:13	 Gene Wood	
v. 10	Dec 26, 2019 14:35	 Gene Wood	Upgrade OIDC identity provide code to fix bug
v. 9	Dec 23, 2019 10:17	 Gene Wood	Adding new Auth0 CA thumbprint
v. 8	Dec 09, 2019 08:35	 Gene Wood	
v. 7	Nov 26, 2019 12:36	 Gene Wood	
v. 6	Nov 22, 2019 09:17	 Gene Wood	
v. 5	Nov 22, 2019 09:11	 Gene Wood	
v. 4	Nov 22, 2019 09:11	 Gene Wood	
v. 3	Nov 22, 2019 09:07	 Gene Wood	
v. 2	Nov 22, 2019 09:05	 Gene Wood	
v. 1	Nov 22, 2019 08:49	 Gene Wood	

Summary & Scope

This document describes how an AWS account owner can enable federated AWS login with Single Sign On (SSO) in their AWS account.

For instructions on how, as an AWS user, to access AWS using your federated single sign on login visit the [How to login to AWS with Single Sign On](#) page

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

AWS Federated Login Account Setup

In order to enable IAM Roles in your AWS account to allow SSO users to assume them, you first have to take the one time step and create an "AWS IAM OIDC Identity Provider" in your AWS account. To do so either deploy this CloudFormation stack with the web UI or on the command line.

Step 1 of 4 : Deploy the AWS IAM OIDC Identity Provider in the web UI

1. Click [this link to launch the "Quick create stack" UI to deploy the identity provider](#)
2. Leave all parameters at their defaults
3. Scroll down and click the I acknowledge that AWS CloudFormation might create IAM resources. checkbox
4. Click `Create Stack`
5. Wait for the stack to finish deploying and resolve to a state of `Create Complete`

If you'd like to deploy the stack using the command line or learn more about the values used in this OIDC identity provider resource, go to the [Advanced Section](#)

To enable users in your AWS account to access AWS resources using their federated login, you'll need to create IAM Roles that permit federated users to assume those roles.

Step 2 of 4 : Determine which user groups to grant access to

The first step is to determine which user groups you want to grant access to assume an IAM Role which those users will use to access resources in the AWS account. An easy way to find out what groups **you** are a member of is by logging in to <https://people.mozilla.org/> then going to your profile and viewing the `Access Groups` section. You can also have your target users visit this page to find out what groups they are a member of. Alternatively you can see what groups you are a member of, in a machine readable format, by visiting <https://sso.mozilla.com/info>

For example, if you wanted to grant access to a team of Mozillians in HR and when those users viewed the list of groups they were a member of it revealed that they were all part of the group called `team_hr` you could use `team_hr` in the next steps to grant them access.

If you want to setup a new group in mozillians.org you'll want to create an "access group" not a "tag" on mozillians.org.

Alternatively, if you want to request that an LDAP group be created for you, [open a bugzilla ticket](#) and request the group be created, the name of the group and the members of the group.

Note : Until [this issue](#) is resolved, keep in mind that all Access Group names in the `Mozillians` section of one's profile don't show the real group name. All Mozillians access groups must be prefixed with `mozilliansorg_` so that for example a mozillians group shown as `foo` would have an actual group name of `mozilliansorg_foo`

Step 3 of 4 : Create an IAM Role

Now that you know the name of the group of users you want to grant access to you can create a pair of IAM roles.

If you'd prefer to craft specific roles with our command line tool, or create your roles by hand, go to the [Advanced Section](#). You can also find more details on this CloudFormation template in the [Advanced Section](#).

1. Click [this link to launch the "Quick create stack" UI to deploy the roles](#). This will create an administrative role and a read-only role.
2. Using the group name you determined above that you wish to grant access to, in the Parameters section, fill in the `Group` value.
3. Scroll down and click the I acknowledge that AWS CloudFormation might create IAM resources. checkbox
4. Click `Create Stack`
5. Wait for the stack to finish deploying and resolve to a state of `Create Complete`

Test your new setup

In order to test and validate your new setup you'll need to do a few things differently than the normal [How to login to AWS with Single Sign On](#) process because the IAM roles have just recently been created. This is because normally IAM roles are scanned for all Mozilla AWS accounts hourly.

1. Force a re-scan of all IAM roles so the system picks up the roles you just created
 - a. Visit <http://aws.sso.mozilla.com/?action=rebuild-group-role-map>
2. Wait a few minutes while the scan runs and collects all federated IAM roles across all Mozilla AWS accounts
3. To make sure that your not using cached values from before this new scan that you just initiated, either
 - a. Run `maws --no-cache`
 - b. Browse to <http://aws.sso.mozilla.com/?cache=false>
4. Assuming that you are a member of the user group that you chose to grant access to the new IAM roles, confirm that the new IAM roles show up in the role picker. Select one and confirm you can access AWS

Step 4 of 4 : Disabling and deleting user roles

Once your users have tested AWS Federated Login, you can begin to remove the individual accounts that are no longer needed. We recommend disabling accounts and their associated keys for a week prior to fully deleting them.

1. Disable users and their associated API keys
 - a. Open up [Identity and Access Management \(IAM\)](#) panel in AWS
 - b. For each user under Users:
 - i. Security Credentials Console password Manage Disable
 - ii. Security Credentials Access keys For each key, choose Make inactive
2. Wait a week to make sure that users or passwords aren't needed, and the inactive API keys don't break any code
3. Delete each user inside IAM, after verifying they and their API keys have not had any activity