Fast Fed

A new standard to simplify sso adoption
Another call for vote on Implementors Draft
Now

Implementors Draft
Up Next

Implementation
Why FastFed?
The Problem
Low adoption of federation in enterprise settings

Why?
It’s hard to configure.
Amazon Web Services cloud application
You must be signed in as a super administrator for this task.
Using Security Assertion Markup Language (SAML), your users can use their Google Cloud credentials to sign in to enterprise-cloud applications.

Set up SSO via SAML for Amazon Web Services
Here’s how to set up single sign-on (SSO) via SAML for the Amazon Web Services® application.

Step 1: Set up Amazon Web Services as a SAML 2.0 service provider (SP)
1. Sign in to your Google Admin console.
   Sign in using an administrator account, not your current account darinmcadams@gmail.com
2. From the Admin console Home page, go to Apps > SAML Apps.
   To see Apps on the Home page, you might have to click More controls at the bottom.
3. Click the Download button to download the Google IDP metadata and the X.509 Certificate.
4. In a new browser tab, log in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
5. In the navigation pane, select Identity providers and then click Create SAML Provider.
6. Select SAML as the Provider Type, and give it a name such as GoogleApps.
7. Upload the IDP metadata you saved earlier from the Google Admin console SAML settings.
8. Click Next and on the following page, click Create.
9. Click the Roles tab on the left sidebar and click Create a New Role to create a role which will define the permissions.
10. Select role name. This name will be displayed next to the login name on the AWS console.
11. Select Role for Identity Provider Access.
12. Select Grant Web Single Sign-On (WebSSO) access to SAML providers. Click Next Step.
13. Leave the Establish trust settings as they are. Click Next Step.
14. Use the Attach policy settings to define the policies your Federated Users will have. Click Next Step.
15. On the following page, review your settings, then click Create the Role.
16. Select your Google service from the identity providers list and note the Provider ARN. This contains your AWS Account ID and the name of the provider (example: arn:aws:iam:ACCOUNT_NUMBER@provider|GoogleApps).
17. Click Save to save the Federated Web single sign-on configuration details.

Step 2: Set up Google as a SAML identity provider (IDP)
1. In a new browser tab, Sign in to your Google Admin console.
   Sign in using an administrator account, not your current account darinmcadams@gmail.com
2. From the Admin console Home page, go to Apps > SAML Apps.
   To see Apps on the Home page, you might have to click More controls at the bottom.
3. Select SAML Apps. If you have SAML configured, click Google IDP.
4. The wizard walks you through the setup. You can copy the Entity ID and the Single Sign-On URL field values and download the X.509 Certificate, paste them into the appropriate service provider setup fields, and then click Next.
5. You can download the IDP metadata, upload it into the appropriate service provider setup fields, and then come back to the Admin console and click Next.
6. In the Basic Application Information window, the Application name and Description values automatically populate.
7. Click Next.

Step 3: Enter the Amazon Web Services specific service provider details in Google Admin console
1. In the Service Provider Details section, enter the following into the Entity ID, ACS URL, and Start URL fields:
   ACS URL: https://signin.aws.amazon.com/saml
   Entity ID: https://signin.aws.amazon.com/saml
   Start URL: Empty
2. Leave Signed Response unchecked.
   When the Signed Response checkbox is unchecked, only the assertion is signed. When the Signed Response checkbox is checked, the entire response is signed.
3. The default Name ID is the primary email. Multi-value input is not supported. You can change the Name ID mapping as per your requirement. Custom attributes of the user schema can also be used after creating them via Google Admin SDK APIs. The custom attributes for the user schema need to be created prior to setting up the Amazon Web Services SAML application.
4. Click Next.
5. Click Add new mapping and map the attribute value
   "https://aws.amazon.com/SAML/Attributes/RoleSessionName" to Basic Information > Primary Email and the attribute value "https://aws.amazon.com/SAML/Attributes/Role" to a custom attribute corresponding to the Amazon Web Services account.
6. In the drop-down list, first select the Category and then choose a User attribute to map the attribute from the Google profile.
7. Click Finish.

Step 5: Verify that SSO is working between G Suite and Amazon Web Services only
Note: Make sure you’re still signed in to the account where Services are configured.
1. Open a G Suite core service, such as Google Calendar.
2. At the top right, click the App Launcher.
3. Scroll to the apps section and click Amazon Web Services.
4. If you are signed in to more than one account, select the Amazon Web Services account is configured.
5. If you configured more than one role, select a role from the list.
6. Click Sign In.
You are signed in to Amazon Web Services.
Lots of Pain

System Administrator
Budget 1-2 weeks to configure SSO to each application

Identity Providers
Each app is different. Custom integration & documentation.

Service Providers
Getting into Identity Provider catalogs. Not self-service.
What should I be doing!?
Today’s Registration Experience

Identity Provider

Copy/Paste

Admin

Copy/Paste

Service Provider
Desired Registration Experience
Learn More

https://www.youtube.com/watch?v=ucQl5p6sa4A
Learn More

https://bitbucket.org/openid/fastfed/src/master/
2 Common FAQs
2 Common FAQs

Question: Does this replace SAML, OIDC, or SCIM?
2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.*
Question: Does this replace SAML, OIDC, or SCIM?

No. It tackles the “44 steps” to setup these technologies.
Also, subsets of each to implement.
2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.*
*Also, subsets of each to implement.*

**Question:** What’s the difference between FastFed and OpenID Federation?
Question: Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies. Also, subsets of each to implement.*

Question: What’s the difference between FastFed and OpenID Federation?

*Solving different problems, but complementary.*
Current Status

We’re building

Iteratively, not big bang.
Current Status

We’re building

Iteratively, not big bang.

Step 1
SCIM
FastFed Enterprise SCIM Profile 1.0 - draft 03
fastfed-scim-1_0

Abstract

This specification defines the requirements to implement the FastFed Profile for SCIM 2.0 Enterprise provisioning. This profile supports continual provisioning, update, and deprovisioning of end-users between the Identity Provider and Application Provider.

Table of Contents

1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
   2.1. Roles and Responsibilities
   2.2. Client Authentication
3. Protocol Extensions
   3.1. FastFed Metadata
       3.1.1. Provisioning Profile URN
       3.1.2. Application Metadata
   3.2. FastFed Handshake
       3.2.1. FastFed Registration Request
           3.2.1.1. Usage of the OAuth-2.0 JWT Profile
       3.2.2. FastFed Registration Response
           3.2.2.1. Usage of the OAuth-2.0 JWT Profile
4. Interoperability Requirements
   4.1. General Requirements
   4.2. User Provisioning
       4.2.1. Create User
       4.2.2. Update User
       4.2.3. Deactivate or Reactivate User
       4.2.4. Delete User
       4.2.5. Get User By Id
       4.2.6. List Users By Alternate Identifier
   4.3. Group Provisioning
       4.3.1. Create Group
       4.3.2. Update Group Metadata
       4.3.3. Deactivate Group
       4.3.4. Delete Group
Current Status

We’re building

Iteratively, not big bang.

Step 1
SCIM
Current Status

We’re building Iteratively, not big bang.

Step 1
SCIM

AWS
Azure
Okta
OneLogin
PingOne
Current Status

We’re building

Iteratively, not big bang.

Step 1
SCIM

Step 2
SAML

AWS
Azure
Okta
OneLogin
PingOne
Current Status

We’re building

Iteratively, not big bang.

Step 1
SCIM

Step 2
SAML

Step 3
FastFed Handshake

AWS
Azure
Okta
OneLogin
PingOne
Current Status

We’re building

Iteratively, not big bang.

Step 1
SCIM

Step 2
SAML

Step 3
FastFed Handshake

Step N
OIDC, Other Profiles, etc...

AWS
Azure
Okta
OneLogin
PingOne
Open Source
Open Source

fastfed4j

GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

About
- Implementation of OpenID FastFed specification in Java
  - Readme
    - Apache-2.0 License
  - Releases
    - No releases published
Open Source

fastfed4j

~80% Complete
12K lines of code (so far)