Fast Fed
A new standard to simplify SSO adoption
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.
   - darinmcadas@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 step on the following page, and 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:saml-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.

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 the IDP, and then click Configure IDP. Select Google IDP.

4. The IDP configuration page appears. The app ID and the single sign-on URL fields are populated.

5. 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.

6. You can also download the IDP metadata, upload it into the appropriate service provider setup fields, and then come back to the Admin console and click Next.

7. In the Basic application information window, the Application name and Description values automatically populate.

8. 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:
   - Entity ID: https://signin.aws.amazon.com/saml
   - ACS URL: https://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 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 4: Enable the Amazon Web Services app

1. Sign in to your Google Admin console.
   - Sign in using an administrator account, not your current account.
   - darinmcadas@gmail.com

2. From the Admin console Home page, go to Security ➔ IAM ➔ Roles ➔ Create new role.
   - To see Security, you might have to click More controls at the bottom.

3. Select Amazon Web Services.

4. At the top right of the gray box, click Edit Service ➔ Amazon Web Services.

5. To apply settings to all organizations, click On for every region, and then click Save.

6. To apply settings to individual organizational units, do the following:
   - At the left, select the organizational unit that contains the role you want to change.
   - To change the setting, select On or Off.
   - To keep the setting the same, even if the parent setting changes.

7. Learn more about the organizational structure.

8. Ensure that your Amazon Web Services user account uses your Google domain.

Step 5: Verify that SSO is working between G Suite and Amazon Web Services

1. Open a G Suite core service, such as Google Calendar.

2. At the top right, click the App Launcher ➔ Amazon Web Services.

3. Scroll to the apps section and click Amazon Web Services.

4. If you are signed in to more than one account, select Services ➔ Amazon Web Services only.

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.

Note: Make sure you're still signed in to the account where Amazon Web Services is configured.
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

Admin

Copy/Paste

Service Provider

Copy/Paste
Desired Registration Experience

Identity Provider

Admin

Service Provider
Learn More

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


668 views • Aug 16, 2019
Learn More

https://bitbucket.org/openid/fastfed/src/master/

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Last commit</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>discussion_artifacts</td>
<td>2019-02-11</td>
<td></td>
<td>Incorporates latest round of feedback...</td>
</tr>
<tr>
<td>html_spec</td>
<td>2020-10-07</td>
<td></td>
<td>Update document revision date</td>
</tr>
<tr>
<td>license</td>
<td>2019-08-28</td>
<td></td>
<td>Add txt version of license</td>
</tr>
<tr>
<td>scenarios</td>
<td>2020-03-08</td>
<td></td>
<td>New SCIM interop profile. Desired...</td>
</tr>
<tr>
<td>text_spec</td>
<td>2020-10-07</td>
<td></td>
<td>Update document revision date</td>
</tr>
<tr>
<td>xml_spec</td>
<td>2020-10-07</td>
<td></td>
<td>Update document revision date</td>
</tr>
<tr>
<td>README.md</td>
<td>631 B</td>
<td>2017-10-17</td>
<td>README.md created online with Bit...</td>
</tr>
</tbody>
</table>
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.*
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.*
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?
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?

*Solving different problems, but complementary.*
Current Status
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

AWS
Azure
Okta
OneLogin
PingOne

Step 2
SAML

Step 3
FastFed Handshake

Step N
OIDC,
Other Profiles,
etc...
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.

Join GitHub today

Implementation of OpenID FastFed specification in Java

About

Readme

Apache-2.0 License

Releases

No releases published
Open Source

fastfed4j

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

Implementors Draft?
Spec Status

Implementors Draft?
Draft
Spec Status

Called for Implementors Draft earlier this year
Spec Status

Called for Implementors Draft earlier this year

8 objections
FastFed Core 1.0 - draft 02
fastfed-core-1_0

Abstract

FastFed simplifies the administrative effort to configure identity federation between an identity provider and a hosted application. The specification defines metadata documents, APIs, and flows to enable an administrator to quickly connect two providers that support common standards such as OpenID Connect, SAML, and SCIM, and allows configuration changes to be communicated directly between the identity provider and hosted application on a recurring basis.

Table of Contents

1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
   2.1. Metadata
   2.2. Endpoints
   2.3. Endpoint Discovery
   2.4. FastFed Handshake
   2.5. User Schemas and Provisioning
      2.5.1. Schema Selection
      2.5.2. Attribute Filtering
3. Metadata
   3.1. Metadata Serialization
   3.2. Metadata Languages and Scripts
   3.3. Provider Metadata
      3.3.1. Capabilities
FastFed Core 1.0 - draft 02

Abstract

FastFed simplifies the administrative effort of managing and deprovisioning users for OpenID Connect, SAML, and SCIM, and allows an administrator to quickly connect to these protocols. This specification defines the requirements to implement the FastFed Profile for SCIM 2.0 Basic 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. Metadata
   2.2. Endpoints
   2.3. Endpoint Discovery
   2.4. FastFed Handshake
   2.5. User Schemas and Provisioning
      2.5.1. Schema Selection
      2.5.2. Attribute Filtering
3. Metadata
   3.1. Metadata Serialization
   3.2. Metadata Languages and Scripts
   3.3. Provider Metadata
      3.3.1. Capabilities
4. Interoperability Requirements
   4.1. General Requirements

FastFed Basic SCIM Profile 1.0 - draft 02

Abstract

This specification defines the requirements to implement the FastFed Profile for SCIM 2.0 Basic 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
Spec Structure

FastFed Core 1.0 - draft 02
fastfed-core-1_0

Abstract
FastFed simplifies the administrative effort provider and a hosted application. The spec enable an administrator to quickly connect OpenID Connect, SAML, and SCIM, and all between the identity provider and hosted app.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
   2.1. Metadata
   2.2. Endpoints
   2.3. Endpoint Discovery
   2.4. FastFed Handshake
2.5. User Schemas and Provisioning
   2.5.1. Schema Selection
   2.5.2. Attribute Filtering
3. Metadata
   3.1. Metadata Serialization
   3.2. Metadata Languages and Scripts
   3.3. Provider Metadata
   3.3.1. Capabilities

FastFed Basic SCIM Profile 1.0 - draft 02
fastfed-scim-1_0

Abstract
This specification defines the requirements to implement the FastFed Provisioning. This profile supports continual provisioning, up 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
   3.2. FastFed Handshake
       3.2.1. FastFed Registration Request
           3.2.1.1. Usage of the OAuth-2.0 JWT Profile
   3.2. FastFed Registration Response
       3.2.2. Usage of the OAuth-2.0 JWT Profile
4. Interoperability Requirements
   4.1. General Requirements

FastFed Basic SAML Profile 1.0 - draft 02
fastfed-saml-1_0

Abstract
This specification defines the requirements to implement the FastFed Basic SAML Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
   3.2. FastFed Handshake
   3.3. FastFed Registration Request
   3.4. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
   4.1.1. SAML Subject
   4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements
Spec Structure

Abstract
FastFed simplifies the administrative effort for provider and a hosted application. The specification enable an administrator to quickly connect OpenID Connect, SAML, and SCIM, and all intermediates between the identity provider and hosted applications.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
   2.1. Metadata
   2.2. Endpoints
   2.3. Endpoint Discovery
   2.4. FastFed Handshake
   2.5. User Schemas and Provisioning
      2.5.1. Schema Selection
      2.5.2. Attribute Filtering
3. Metadata
   3.1. Metadata Serialization
   3.2. Metadata Languages and Scripts
   3.3. Provider Metadata
      3.3.1. Capabilities
4. Interoperability Requirements
   4.1. General Requirements

Objections

Abstract
This specification defines the requirements to implement the FastFed Basic SCIM Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
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

FastFed Basic SAML Profile 1.0 - draft 02
fastfed-saml-1_0

Abstract
This specification defines the requirements to implement the FastFed Basic SAML Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
      3.1.1. Authentication Profile URN
      3.1.2. Application Metadata
   3.2. FastFed Handshake
      3.2.1. FastFed Registration Request
      3.2.2. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
      4.1.1. SAML Subject
      4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements
Naming Confusion

FastFed Basic SAML Profile 1.0 - draft 02
fastfed-saml-1_0

Abstract
This specification defines the requirements to implement the FastFed Basic SAML Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
      3.1.1. Authentication Profile URN
      3.1.2. Application Metadata
   3.2. FastFed Handshake
      3.2.1. FastFed Registration Request
      3.2.2. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
      4.1.1. SAML Subject
      4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements
Confusing

FastFed Basic SAML Profile 1.0 - draft 02
fastfed-saml-1_0

Abstract
This specification defines the requirements to implement the FastFed Basic SAML Profile.

Table of Contents

1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
       3.1.1. Authentication Profile URN
       3.1.2. Application Metadata
   3.2. FastFed Handshake
       3.2.1. FastFed Registration Request
       3.2.2. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
       4.1.1. SAML Subject
       4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements
Confusing

Naming Confusion

Abstract
This specification defines the requirements to implement the FastFed Basic SAML Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
      3.1.1. Authentication Profile URN
      3.1.2. Application Metadata
   3.2. FastFed Handshake
      3.2.1. FastFed Registration Request
      3.2.2. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
      4.1.1. SAML Subject
      4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements

Abstract
This specification defines the requirements to implement the FastFed Enterprise SAML Profile.

Table of Contents
1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Overview
3. Protocol Extensions
   3.1. FastFed Metadata
      3.1.1. Authentication Profile URN
      3.1.2. Application Metadata
   3.2. FastFed Handshake
      3.2.1. FastFed Registration Request
      3.2.2. FastFed Registration Response
4. Schema Binding
   4.1. SCIM-to-SAML Attribute Mapping
      4.1.1. SAML Subject
      4.1.2. SAML Attributes
   4.2. Privacy Considerations
5. Interoperability Requirements
   5.1. Identity Provider Requirements
   5.2. Application Provider Requirements
SAML Subject
SAML Subject

BEFORE

“MUST be the username”
SAML Subject

BEFORE

“MUST be the username”

NOW

Configurable
As a reference to implementors, the following considerations can be taken into account when choosing a SAML Subject:

- The format of externalId is defined in section 3.1 of the SCIM Core specification [RFC7643]. It is a persistent identifier, often a GUID, which is intended to reliably identify a user within the Identity Provider. However, it will vary between Identity Providers. Therefore, if an App uses externalId, it must be aware that it may need to handle different identifiers as a result of changes in identity providers. For example, if the App needs to switch Identity Providers, it must ensure that the externalId is consistent across providers.

- The format of userName is defined in section 4.1.1 of the SCIM Core specification [RFC7643]. It is a displayable, user-friendly identifier for a user. In practice, the userName can often be an email, but other formats occur. No assumptions should be made about the format of the(userName) value other than that it is a string that the end-user typically enters as a login when authenticating.

- If the Administrator switches Identity Providers, it is usually the case that the userName remains consistent across providers, making it easier to correlate authentication and provisioning events to a single user when events are arriving from different sources.

- Note that userName is mutable, meaning an end-user can change their userName. In addition, userName can be recycled and reassigned to other end-users. Therefore, Applications should consider how such situations will be handled. The ability to be notified when userName is changed or recycled, such as via the SCIM profile [FastFedProfile.EnterpriseSCIM], can help keep an Application Provider up-to-date with changes.

- The attribute "emails[primary eq true].value" represents the primary email address of the user, where emails is defined in section 4.1.2 of the SCIM Core specification [RFC7643].

- If an end-user does not have a value for email defined within the Identity Provider, the end-user will be unable to authenticate to the Application. As a result, choosing email as a SAML Subject is appropriate only when an Application requires an email address and is willing to reject end-users who lack it.

- In addition, emails can be changed or recycled in the same manner as the userName. Therefore, similar mechanisms are necessary to handle such events.

- In some circumstances, it may be necessary to use multiple attributes to best match a SAML Authentication response against a specific end-user in the Application. If this occurs, it is acceptable to use both the SAML Subject and the SAML Attributes in combination to perform the matching. In this scenario, the choice of SAML Subject becomes somewhat flexible, and one may choose whichever option is most likely to be available and useful.
Up Next

Another call for vote on Implementors Draft