Overview of FastFed Scenarios

FastFed can solve a variety of SSO configuration scenarios. This document enumerates the scenarios in scope. It includes business context and user experience.

As per discussion at the 10/25/18 meeting, the working group priority is Scenario #1, starting with SSO configuration only. This will be followed by de-provisioning and then provisioning.

The remaining scenarios will be addressed in the fullness of time.

# Scenario 1) Existing Application - Convert to SSO

**Synopsis**

One or more members of an organization are using an online application. Corporate IT discovers the usage and wants to convert the application to SSO with automatic user lifecycle management.

This conversion can happen iteratively by first enabling SSO, then later enabling provisioning. Alternatively, both steps can happen concurrently in a big-bang migration. Both variations are covered in this scenario.

**Example Business Context**

Alice works at an employer named Company.com. She discovered a tool at OnlineService.com that helped her be more productive. Without asking permission, she registered on OnlineService.com with a work email (“alice@company.com”) and created yet-another password for signing in to OnlineService. She used her personal credit card and submitted expense reports for the cost.

Alice enjoyed the service and invited co-workers to collaborate. To do so, she visited a UI at OnlineService.com and sent invitations to others. The invitation form asked for an email, so she entered “bob@company.com” plus dozens more coworkers. Each recipient received an email with a registration link. When clicking the link, they were prompted to create their own profile and passwords with OnlineService.com.

Eventually, Corporate IT at Alice’s company noticed widespread use of the unapproved online service. They audited the service and although some aspects concerned them, usage was entrenched and too disruptive to stop. So, they aimed to put the best security controls in place.

Part of those controls include gating who at Company.com can access the product and revoking access when appropriate.

To enable this, Corporate ID has three goals. First, they want to enable single sign-in via the company IdP. Second, they want to provision users based on an access-control system (e.g. groups in a directory) that grants only the right persons access to the Online Service. Third, they want lifecycle controls so user sessions and accounts can be reaped when users no longer have access to the service, such as upon termination of employment.

Due to the complexity of the migration, Corp IT may execute iteratively. First, they enable SSO. Second, they enable life cycle management and provisioning. Alternatively, Corp IT may choose to execute both steps concurrently in a big-bang migration.

All the variations are illustrated below.

**User Experience**

*Variation A) Enabling both SSO & Provisioning at the same time*

1. Alice signs-in to OnlineService.com and navigates to the page for configuring SSO.
2. [Optional] If Alice’s employer, Company.com, has enabled FastFed Discovery:
   * Alice sees her company name and logo with a button inviting her to configure SSO with company credentials.
   * Alice clicks the button and jumps to Step #6 below.
3. If automatic discovery is not available, Alice sees a page of instructions:
   * The instructions tell Alice to gather information from her IT Department, including a FastFed URL if available.
   * If Alice gets a FastFed URL:
     + Alice returns to OnlineService.com to finish configuring SSO.
     + Alice enters the “FastFed URL” in a text box. OnlineService validates the information and if everything is OK, Alice sees her company name and logo with a button inviting her to configure SSO. Alice clicks the button.
   * Otherwise, without a FastFed URL:
     + The instructions fallback to manual configuration (without FastFed). E.g. uploading SAML metadata files. This flow ends.
4. Alice is redirected to a page hosted by her company’s identity provider.
5. Alice may be prompted to sign-in to the Identity Provider.
6. The next steps vary, depending on whether Alice has administrative permissions in the IdP to finish configuring SSO & Provisioning. This depends on the capabilities and policies of her company and the IdP.
   * If Alice DOES NOT have permissions, she may see a button to enqueue the request to her local IT team for approval. The IT team executes the remaining steps.
   * If Alice DOES have permissions, no interruption occurs and Alice immediately proceeds to Step 9.
7. A UI page hosted by the IdP displays the proposed configuration for SSO and Provisioning. This includes:
   * The target application name and logo (e.g. “OnlineService.com”)
   * User data that will be provisioned into the application, such as Name, Email Address, etc.
8. If the proposed SSO configuration is acceptable, the end-user clicks a button to approve.
9. Upon submission, the end-user sees a confirmation page hosted by the IdP showing that SSO and Provisioning are now enabled.
10. At this point, the configuration is complete. However, there may be additional work to complete the transition. For example, the administrator may wish to deactivate all the old password credentials on OnlineService.com. They may also need to give hints to the service provider regarding how to match incoming SSO sessions with one of the existing users in the system (e.g. match on email address? Or something else?)  
    These details are outside the scope of FastFed and can vary by service provider.

*Variation #B) Enabling SSO first, then adding User Provisioning later*

* This is largely the same as Variation (A) except that Alice performs the sequence of operations twice.
* On the first pass:
  + OnlineService.com gives Alice the option to only enable SSO (no provisioning). Alice selects this option.
* On the second pass:
  + OnlineService.com asks Alice whether she wants to modify the existing configuration or create a new one. Alice chooses “modify” and is presented the option to turn on provisioning. She selects this option.

# Scenario 2) Existing Application – Invite External Party

**Synopsis**

The administer of an online application wants to enable SSO for external parties who don’t exist in the same directory as the administrator. This can occur when collaborating with external business partners, or in subsidiary/franchisee scenarios where a parent organization invites sub-entities to use parent company resources.

**Example Business Context**

Alice has completed scenario #1 (above). She and her fellow employees are using SSO when accessing OnlineService.com.

As part of her job, Alice interacts with suppliers. Alice would like to invite suppliers to collaborate with her in the Online Service. Alice checked with her security team and they approved sharing the data.

Alice could invite the suppliers to create local accounts with the Online Service, using yet-another username and password. However, she has concerns. First, there has been a lot of employee turnover at the supplier and she is worried about having to frequently add/remove users. That’s a hassle. Alice would prefer for her point of contact at the partner organization to control who should work on Alice’s application, perhaps via group membership in the partner’s directory, and those parties are automatically added/removed to Alice’s application without her involvement. (Alice has locked down permissions appropriately in her application so that the suppliers can only perform the tasks she has contracted them to perform, and no more.)

In addition, from the supplier’s perspective, they are accustomed to SSO and would prefer it, rather than having another password just for working with Alice’s company.

Therefore, Alice wants to invite an external company to SSO into her instance of OnlineService.com, with user lifecycle management that is controlled by the partner organization.

**User Experience**

This flow involves two personas: Alice, the application owner, and Paul, her point of contact at the partner company.

1. Alice signs-in to OnlineService.com and navigates to the page to “Share with Others”.
2. Alice sees a new option to connect with a business partner.
3. Alice choses this option and sees an interview-style wizard that asks a sequence of questions. The first question it asks is whether Alice has an email address for her external partner.
4. Alice enters the email: “paul@partner.com”
5. [Optional] If Alice’s partner company has enabled FastFed Discovery:
   * Alice sees her partner company’s name and logo with a button inviting her to enable SSO.
   * Alice clicks the button and jumps to Step #9 below.
6. If automatic discovery is not available, Alice sees a page of instructions:
   * The instructions tell Alice to gather information from her partner.
   * The instructions ask the partner if they have a “FastFed URL” available.
   * If not available, the instructions fallback to traditional hand-configuring SSO, e.g. exchanging SAML Metadata. FastFed is not used. This flow ends.
7. Paul follows the instructions, gathers his FastFed URL, and emails it to Alice.
8. Alice returns to OnlineService.com, and enters Paul’s email address and FastFed URL. OnlineService validates the information and if everything is OK, Alice sees her Paul’s company name and logo with a button inviting her to configure SSO. Alice clicks the button to proceed.
9. An email is sent to “paul@partner.com” with a link.
10. Paul receives the email and clicks the link. This opens a page hosted by his company’s identity provider.
11. Paul may be prompted to sign-in to his Identity Provider.
12. The next step varies, depending on whether Paul has administrative permissions in the IdP to finish configuring SSO. This is outside the scope of FastFed and depends on the capabilities and policies of his company and the IdP.
    * If Paul DOES NOT have permissions, he may see a button to enqueue the request to his local IT team for approval. The IT team would execute the remaining steps of this flow.
    * If Paul DOES have permissions, no interruption occurs and Paul immediately proceeds to Step 13.
13. A UI page hosted by the IdP displays the proposed SSO configuration. This includes:
    * The target application name and logo (e.g. “OnlineService.com”)
    * The employee data that will be provisioned to the application. This depends on the application, but may include the user’s name and email address.
14. If the proposed SSO configuration is acceptable, the user clicks a button to approve.
15. Upon submission, the end-user sees a confirmation page showing the relationship is now enabled.
16. Both Paul and Alice receive a confirmation email.
17. Paul can then edit the settings in his IdP to control which employees get access to Alice’s application instance.

# Scenario 3) New Application - Enterprise Onboarding

**Synopsis**

This is a greenfield scenario where a large enterprise is onboarding to an application and seeks to provision users and enable SSO from day one, before anyone uses the service.

Note - In order to explore the upper bound on complexity, this scenario uses an example of an HR/Payroll service company. This is a feature-rich use case for FastFed as it necessitates an extended schema and user lifecycle management that stretches from pre-employment to post-employment.

**Example Business Context**

Alice has acquired a reputation as a domain expert with 3rd party application integrations. Therefore, Alice’s peers in Corp IT have requested her help with a major new initiative. The company has selected a new provider named “ADZ” to handle all payroll for the company. Alice is asked to assist with onboarding.

The goal is to pre-provision all employees into the application and enable SSO.

Alice visits the ADZ.com home page but there isn’t a regular sign-up link. Instead, she must submit a request to talk to an account representative. Fortunately, someone in Corp IT has already established this relationship, negotiated pricing, and signed a contract. That person listed “alice@company.com” as the technical point of contact.

While ink dries on the contract, Alice receives an auto-email inviting her to finish integrating her company with ADZ.com. Alice clicks the link and is prompted to create an administrator account and password on ADZ.com. Alice wishes she could use SSO immediately rather than creating a password, but she postpones that feedback for later and proceeds to create her account. (See Scenario #4 for an example of SSO at sign-up.)

Alice then navigates to the page to configure SSO and user provisioning. At this point, Alice realizes this application is somewhat unique. New employees interact with ADZ.com *\_before\_* their start date of employment, to submit tax paperwork and such. And, they interact with ADZ.com *\_after\_* employment ends, for tax documents and historical payroll information. During these bookend periods, the individual won’t have any corporate credentials; they can only authenticate with personal credentials or social media accounts. In the middle period of employment, they may SSO with corporate credentials. (Some companies choose to mandate this.)

Another complexity is that “EmployeeID” is the only static identifier throughout this lifecycle. In contrast to other applications that are satisfied by using an “email address” to identify users, the users of ADZ.com won’t have a corporate email address until their start date arrives. And, if the person leaves the company, that corporate email address could be reused, making it an unreliable key for long-term identification of an individual.

After consulting with her HR department and ADZ online documentation, Alice advises her Corp IT team to represent users in their directory based on the SCIM “EnterpriseUserExtended” schema. (Editor’s Note: That schema doesn’t exist today. Placeholder.) That schema extends the default EnterpriseUser schema with additional attributes needed for full employee lifecycle management by HR and Payroll applications. This includes fields like StartDate, EndDate, Employment Status, etc…. (TODO – research if there is truly a common set of attributes.)

With this in place, the remaining integration steps become straightforward with FastFed.

**User Experience**

Same as Scenario #1, Variation 3.

However, behind-the-scenes, the flows may be more complicated due to the extended schemas and richer provisioning.

# Scenario 4) New Application - Individual Sign-Up with SSO

**Synopsis**

In this scenario, individuals sign-up to an online application with their organizational identity and credentials. This is similar to the consumer experience for signing-up to an application using Google or Facebook accounts, but applied to the enterprise environment.

**Example Business Context**

Alice has discovered another online service (AnotherService.com) with potential to be useful. If Alice likes the application, she may share it with others. But, at this point, she wants to kick the tires on the product. Fortunately, the product has a free tier for introductory usage.

Alice would like to sign-up with AnotherService.com. However, based on her prior experience, she understands the value of SSO and would like to leverage her existing corporate profile to sign-up, rather than creating yet-another account and retyping all her user information.

Alice also built a good relationship with her security team and convinced them it’s better to permit employees to use SSO from day one with online applications. Otherwise, employees create shadow IT. Therefore, the security team has enabled self-service “auto-registration” of 3rd party applications within the corporate identity provider. The security team may have policies or whitelists/blacklists of applications trusted for auto-registration.

**User Experience**

* Alice visits the home page of AnotherService.com and clicks “Sign-Up”.
* On the sign-up page, Alice enters the email [alice@company.com](mailto:alice@company.com)
* [Optional] If Alice’s company has enabled FastFed Discovery for self-service:
  + Alice sees her company logo with a button inviting her to sign-up with her company account.
  + Alice selects the option to sign-up with her company account.
  + Alice is redirected to a page hosted by her company’s identity provider. It displays the data that will be released to AnotherService.com, such as Alice’s name and email. Alice is asked for confirmation.
  + Alice clicks a button to approve and is redirected back to AnotherService.com.
  + At this point, Alice is signed-in and her user information is prepopulated into AnotherService.com.
* If automatic discovery is not available, Alice signs up manually with a password.