SAP Fieldglass

PUBLIC
SAP Fieldglass
2020-12-13

Single Sign-On (SSO) Configuration Guide

THE BEST RUN SAP

Content

1 Introduction

Single sign-on allows users to access SAP Fieldglass using their corporate credentials.

The primary purpose of this document is to communicate the feature functionality and preferred approaches to implement Single Sign-On with SAP Fieldglass. With SSO, an end user logs into their internal, corporate identity management system—often referred to as a "Federation" system—and is then able to access external systems without the need for entering further credentials specific to that external system. There are several advantages to implementing SSO, including:

- Simplifying end users sign-on operations and reducing time spent by users managing their credentials.
- Reducing IT costs by lowering help desk calls related to username/passwords issues.
- Improving security on all levels of access to systems without the need to re-prompt users for authentication.

The SAP Fieldglass SSO feature provides customer users with the option to connect to the application via SSO or by logging in with a user name and password, outside of SSO. Customer users can be configured to restrict to login via SSO only or enable both access options. This design allows flexibility for users to securely access their SAP Fieldglass information at anytime via their corporate network or over the internet.

2 Implementing SSO

Before implementing SSO, there are technical, user, and access considerations considerations that must be addressed.

Technical Compatibilty

Before beginning actual implementation of SSO with SAP Fieldglass, technical compatibility should be analyzed and confirmed. SAP Fieldglass SSO implementations will be OASIS standard SAML exchanges, securely transmitted over HTTPS. SAP Fieldglass supports both IdP- and SP-initiated SSO, providing different options and advanced capabilities. More technical specifications can be found throughout this document.

Users

The first step in implementing SSO in SAP Fieldglass is aligning the user populations between the client's Federation system and SAP Fieldglass. It should be determined which unique identifier from the Federation system will be used to identify the user during the SSO login process, which will often times be an employee ID or email address. Once determined, the users in SAP Fieldglass will need to be configured to match that identifier, so that a successful login can occur.

Certificate

The other main component of the implementation is obtaining the SAML signing certificate (a PKI certificate) from the customer and loading it into the SAP Fieldglass application. This certificate is used to sign the SAML message sent from the Federation server to Fieldglass during a login attempt. When consuming that message, the SAP Fieldglass server matches up the certificate from the SAML message to the one that is loaded and verifies that the SSO request came from the client.

Access

From there, one additional step that the customer will complete is to configure an internal link on their portal, which will allow users to initiate an SAP Fieldglass session (sessions might also be initiated out of notification emails sent from SAP Fieldglass, aka "Deep Linking", but this internal link will allow for opening sessions at will). The link can then be used to verify a successful SSO implementation—if everything checks out, the user should be directly logged into the application (if not, they will end up at the SAP Fieldglass landing page with an error message on the

screen). Once they are done with their session, they can press the “Log Out” button and either the window will be closed or the user will be redirected to another URL, based on how the client has configured their SSO call.

3 Configuration Considerations

Before implementing SSO, there are several business scenarios that should be considered to ensure success.

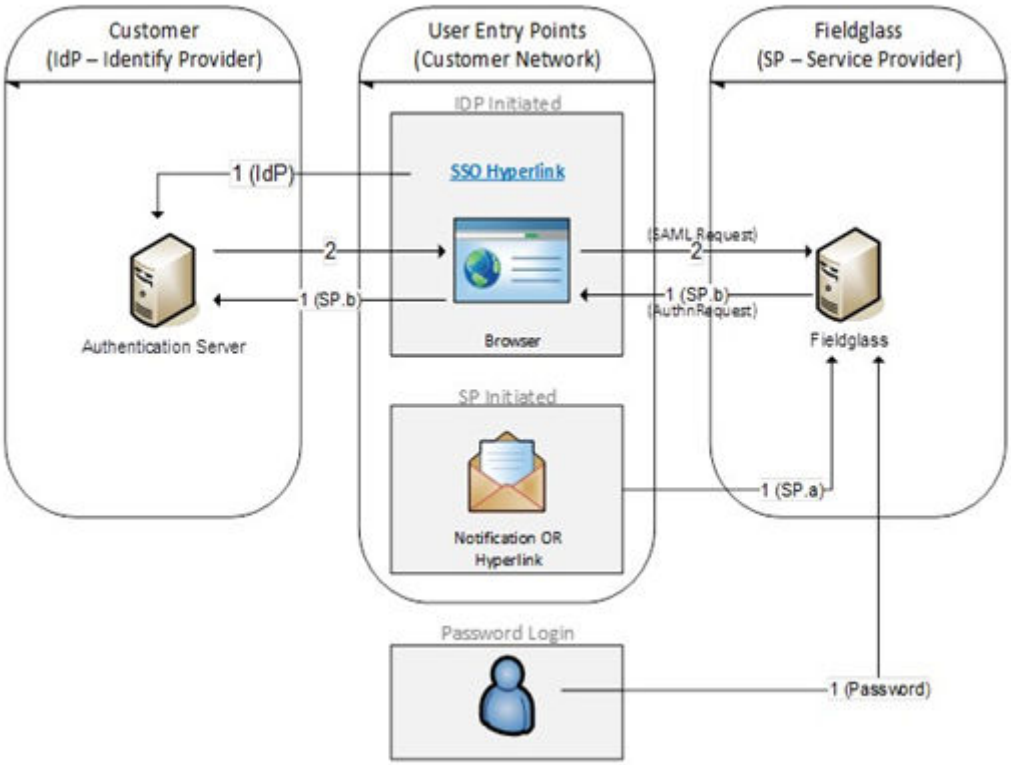
The following questions should be evaluated prior to implementing SSO.

Question	Proposed Solution or Recommendation
Are in-house technical skills required on the customer side?	Technical resources will be required to deploy SSO and the knowledge areas include Public/Private Keys, SAML Post (1.1 or 2.0) and encryption algorithms. If there are no internal resources with this expertise, external resources can add extra costs to the project.
What identifier will be used for the user?	Typically, a company employee ID or email address will be used as the SAP Fieldglass username. If an employee ID is used, a buyer code suffix will need to be appended to the end of the username to ensure uniqueness within SAP Fieldglass (ex. "123456789_ABC" where 123456789 is the employee ID and the company code = ABC).
Will users only login through SSO or will they have SSO and username password access?	This configuration decision is dependent on the business requirements and may vary based on the user role.
Will there be users that will only login through username password only?	There may be a need to provide certain users with direct login (username/password) capability. The list of users that require direct login (username/password) access should will be supplied before deploying SSO in production.
What is the volume and frequency of changes to the user base?	As users are added, updated and removed from the Customer system, corresponding changes must also be made in SAP Fieldglass. If the usernames are not synchronized, SSO authentication may fail due to mismatches.
How are new users introduced to SAP Fieldglass handled?	All new users to SAP Fieldglass will inherit the SSO setting, as set at the company configuration level. Newly created users will not receive a user invitation if the company is configured for SSO Only. They are allowed to login for the first time via SSO. No registration is required (as in the username/password email registration process).

4 Process Flow

Depending on user entry points, there are multiple authentication workflows in SAP Fieldglass.

The following diagram depicts the authentication workflows for user entry points within SAP Fieldglass.



1. Session Initiation
   IdP (IdP-Initiated Session): User clicks an internal hyperlink, which points directly to internal application/ authentication server, for internal user authentication.
   SP (SP-Initiated Session)
   1. User clicks a link from an SAP Fieldglass notification or login URL, which points directly to SAP Fieldglass.
   2. SAP Fieldglass receives request and sends “AuthnRequest” back to the customer’s authentication server via user’s browser, for internal user authentication.

   Password (Optional Login/Password Session) - Username and password can be created and utilized in addition to SSO access. Password registration required.
2. SAML Request
   Once the user is authenticated by the customer’s internal authentication server, a SAML request (aka “SAML assertion”) is sent to SAP Fieldglass via the user’s browser. The SAP Fieldglass authentication process then occurs.

5 Technical Specifications

SAP Fieldglass administrators using SSO require several specifications for proper implementation.

Specification	Definition
General Information	
Signing Certificate (PKI)	Customer supplied. Used to Sign the SAML Assertion. Pre-stored in SAP Fieldglass System. Base64 format preferred.
Web Session	Tracking Cookie = JSESSIONID Timeout = 15 minutes
Metadata	Production metadata enclosed in the Metadata and Sample Files section.
Fieldglass ACS URL	
ACS URL	SAP Fieldglass: https://www.fieldglass.net/SSOLogin?SSO-Params=company%3DABCD%3B%3Breturningurl%3Dclose-Window SAP Fieldglass Flex: https://flex.fieldglass.net/SSOLogin?SSOParams=company%3DABCD%3B%3Breturningurl%3DcloseWindow
Domain	SAP Fieldglass • Production - https://www.fieldglass.net • Test - https://xuat.fgms.com SAP Fieldglass Flex • Production - https://flex.fieldglass.net • Test - https://flexeuat1.fgvms.com
Parameter 1 (company)	Company code, as defined in SAP Fieldglass (e.g. ABCD)
Parameter 2 (returningurl)	URL to redirect user to on logout or "closeWindow"
SAML	
Profile	SAML POST
Version	SAML 1.0, SAML 1.1 and SAML 2.0 are supported
SP-Initiated Configuration Items (Optional)	

Specification	Definition
IdP URL	Customer supplied. Destination for AuthnRequest
HTTP Methods Supported	POST or GET
HTTP Parameters	Customer supplied, if needed.
Login URL	SAP Fieldglass: https://www.fieldglass.net/SSOLogin?TARGET=company%3DABCD SAP Fieldglass Flex: https://flex.fieldglass.net/SSOLogin?TARGET=company%3DABCD
Domain	SAP Fieldglass • Production: https://www.fieldglass.net • Test (subject to change): https://xuat.fgvms.com SAP Fieldglass Flex • https://flex.fieldglass.net • Test (subject to change): https://flexeuat1.fgvms.com
Parameter 1 (company)	Company code, as defined in SAP Fieldglass (e.g. ABCD)
AuthnRequest	
Protocol Binding	HTTP POST or REDIRECT
Signed Request	Optional
“ProviderName” attribute*	SAP Fieldglass Default: https://www.fieldglass.com SAP Fieldglass Flex Default: https://flex.fieldglass.com
“Destination” attribute*	Default: IdP URL, as configured in FG (from field above)
“AssertionConsumerServiceURL” attribute*	Default: Not included.
<Issuer> element*	SAP Fieldglass Default: https://www.fieldglass.com SAP Fieldglass Flex Default: https://flex.fieldglass.com

* Customized value available upon request.

6 Frequently Asked Questions

Frequently asked questions about SSO in SAP Fieldglass.

Question	Answer
Is the signing certificate required as a part of the SAML response in XML?	No, the signing certificate must be preloaded.
Is a custom SAML login failure page or re- direct to a provided URL available, if the SAML assertion is either expired or invalid?	This is not currently supported by the SAP Fieldglass SSO solution.
What are your SAML login tracing and auditing features?	SAP Fieldglass maintains an audit trail of SAML user logins. This information is available for query by SAP Fieldglass Flex technical engineers.
Does SAP Fieldglass support Deep Linking?	SAP Fieldglass supports deep-linking with SP-initiated, HTTP-POST specifications are based on the Profile for OASIS SAML standards. Section 3.5 of the Binding for OASIS SAML details HTTP POST Binding standards. This is utilized for email notifications of work items.
Can SAP Fieldglass provide a Metadata link?	A specific URL cannot be provided; however, detail is enclosed within the Metadata and Sample Files section of this document.

7 SSO Glossary

There are several terms that SAP Fieldglass administrators should be familiar with during implementation of SSO.

Term	Definition
ACS URL	Assertion Consumer Service URL. Endpoint where service provider will receive assertion.
HTTPS	Hypertext Transfer Protocol over SSL (Secure Socket Layer). It is a TCP/IP protocol used by Web servers to transfer and display Web content securely. The data transferred is encrypted so that it cannot be read by anyone except the recipient.
IDP	Identify Provider - The application that takes authentication information (commonly a username and password) and translates that into identity information (name, email, etc.) which it provides to Service Providers based on defined policies.
IDP Destination URL	Federation Server URL provided by IDP for Service Provider (SP) initiated requests.
PKI Certificate	Federation Server URL provided by IDP for Service Provider (SP) initiated requests.SAML - Security Assertion Markup Language (SAML) is an XML-based solution for exchanging user security information between an enterprise and a service provider.
SAML	Security Assertion Markup Language (SAML) is an XML-based solution for exchanging user security information between an enterprise and a service provider.
SP	Service Provider (SAP Fieldglass) - An application that provides service to the end user. The software that provides some access control and communicates with the IDP for identity information.
SSO	Single Sign-On - A process whereby credentials are entered only once and allow access to separate systems without having to re-authenticate for the duration of the session.

8 Metadata and Sample Files

SAP Fieldglass provides standard metadata for administrators implementing SSO. Other sample files are available upon request.

Metadata

Below is the standard metadata for SAP Fieldglass. It is mostly complete, though should be updated to match the given implementation; that is, to point to the appropriate SAP Fieldglass environment and call out the client's company code. This is done by updating the "Location" attribute of the <AssertionConsumerService> element as such:

- The domain of the URL should be updated to match the corresponding environment in SAP Fieldglass (production domain given below, others might be something like 'xcore3.fgvms.com', for example). For SAP Fieldglass Flex, the location URL should be updated to match the corresponding test environment in SAP Fieldglass Flex ('https://flexeuat1.fgvms.com', for example).
- The 'company' parameter within the URL should be updated with the company code assigned within SAP Fieldglass.

SAP Fieldglass Metadata Sample

Sample Code

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
entityID="https://www.fieldglass.com">
    <SPSSODescriptor AuthnRequestsSigned="false"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
NameIDFormat>
    <AssertionConsumerService isDefault="true" index="0"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.fieldglass.net/SSOLogin?SSOParams=company%3DXXXX%3B%3
Breturningurl%3DcloseWindow">
    </AssertionConsumerService>
    </SPSSODescriptor>
</EntityDescriptor>
```

SAP Fieldglass Flex Metadata Sample

Sample Code

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="https://
www.fieldglass.com"xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:
2.0:protocol"
WantAssertionsSigned="true" AuthnRequestsSigned="false">
```

```
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified</
NameIDFormat>
<AssertionConsumerService
Location="https://flex.fieldglass.net/SSOLogin?SSOParams=company%3DXXXX%3B
%3Breturningurl%3DcloseWindow"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" index="0"
isDefault="true"/>
</SPSSODescriptor>
</EntityDescriptor>
```

SAML and AuthnRequest Sample Files

SAML assertion and AuthnRequest examples available upon request.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP