Single Sign On – Customer Guide

Document History

Version	Change	Author	Date
0.1	Document Creation	Tim Day/Suhail Adam	January 10th 2022

Table of Contents Page Number

Introduction	4
Safeguard and Auth0	4
Key Steps	4
Our Underlying Technology	5
Implementing SSO	5
Key Attributes	6
Support	6

Introduction

Single Sign On (sometimes known as Federated Identity) is the creation of a trusted connection between the Customer Identity System ("IDP") and Safeguard's Global Unity System ("Global Unity"). It enables the following:

- A simple method for customer users to authenticate with the Global Unity system without the need to enter credentials, therefore providing user convenience
- An authentication gateway that enables Customers to centrally control which employees have access to Global Unity; new employees and terminations can have their access centrally managed by the Customer IDP.
- Enforcement of Customer Security Controls such as leveraging Multi-Factor Authentication ("MFA") (a process where a one-time code is required to complete a login to a third party system) to be used therefore keeping third party system accesses consistent with a company's security policies and controls
- It prevents the users from needing to maintain login credentials to third party systems

Safeguard & Auth0

Safeguard uses Auth0 as it's IDP.

Once authenticated via SSO, Safeguard has a pass-through SSO Implementation in place to enable customers to access Zendesk & Global Unity, as can be seen below.

Therefore, the customer implementation is to Safeguard's Auth0 tenant.

Key Steps

There are some fundamental steps involved in creating the trust relationship between the customer IDP and Global Unity. Additionally, there are other considerations that should be explored and planned as part of the implementation. Once the solution is live, maintenance should be minimal, If you require any help then please follow the support process. We'll address that later in this article.

The key steps are:

1. Implement SSO between Customer IDP and Safeguard Global

2. Manage Authorisations within Global Unity

3. Communicate the service to your applicable users

4. Ensure support is in place

Our Underlying Technology

Whilst the Global Unity system is a proprietary application owned by Safeguard Global, Safeguard Global has taken the decision to use Auth0 as their own IDP. Therefore, integrations from customer IDPs such as Okta, Ping, Auth0, ADFS, Azure and other SAML 2.0 based identity systems will need to be integrated with the Safeguard Global Auth0 tenant.

In all cases the SAML 2.0 standard is followed for creating trusted connections between Customer and Safeguard IDPs.

Implementing SSO between Customer IDP and Safeguard Global's Global Unity system

The customer will require the following details from Safeguard Global to enter into their IdP :

- The **Entity ID**: urn:auth0:prodsafeguard:YOUR_CONNECTION_NAME
- The **Post-back URL** (also called Assertion Consumer Service URL): https://auth.safeguardglobal.com/login/callback?connection=YOUR_CONNECTION_NAME

The YOUR_CONNECTION_NAME will be set up and sent by the customer to the Safeguard Global support team.

To connect to Safeguard Global applications using SAML, Safeguard Global needs the below information from the customer:

1. SAML login URL
2. SAML logout URL (optional)
3. X.509 signing certificate
4. Issuer ID / Entity ID / Idp ID (all mean the same thing) [e.g. https://sts.windows.net/1234abcd-78we-34sj-78hj-123456abcdefg/

Once the customer has this information, it needs to be sent to the following email address: SSOsupport@safeguardglobal.com

Key Attributes

The following attributes should be passed in the request sent by the customer IDP.

Attribute 1: EMAIL

Email Addresses must be consistent between customer IDP and Safeguard records. If the email address supplied is not the email address that Safeguard Global have on there records the set up will be unsuccessful.

Attribute 2: NAME

The NAME attribute has to be the full name of the employee.

Support

If you any issues arise or help is required with the implementation of SSO please get in touch with Safeguard by raising sending an email to **SSOsupport@safeguardglobal.com**. Please include the following information:

- Customer Name
- Full Employee Name of the user experiencing the issue
- Email address of the employee
- Description of the error and any screenshots if applicable.

The support team will then get in contact with you.

End of Document