Silverfin Single Sign-on

1. Introduction

This document is meant for the technical department of Silverfin customers. It explains how Single Sign-on can be setup with Silverfin. The details this document describes are based on the situation on *26/01/2018.*

2. Generic

Setting up Silverfin with Single Sign-on means authentication to the Silverfin application will be handled by another party. This allows you to set custom password rules (renewal, complexity), enable multi-factor based on location or setup any other authentication specific setting.

Silverfin currently supports three types of Single Sign-on (SSO):

- AzureAD
- OpenID Connect
- OpenID *(deprecated)*

Independent of the solution used for SSO, enabling SSO for a user in Silverfin has these implications:

- User cannot login with username password anymore
- Silverfin password restrictions don't apply to this user anymore
- User cannot reset password in Silverfin anymore

Environments on SSO are configured with a subdomain, to allow for deeplinking and automatic redirection to the SSO provider.

3. AzureAD

AzureAD[1] is the standard online authentication provider from Microsoft. AzureAD can be configured as a slave of an on premise Active Directory installation, so it's easy to extend credentials being used iternally already.
To configure AzureAD with Silverfin, you only need to provide the email domain you want to use with Silverfin, we can setup the rest.

[1] https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis

4. OpenID Connect

OpenID Connect (OIDC)[2] is a standard authentication mechanism built on OAuth 2.0. It must not be confused with OpenID, which is a completely different (legacy) protocol. Silverfin can be configured as an OIDC client, so you would need to implement an OIDC provider. To setup OIDC, you need a callback url from Silverfin, which typically looks like https://*someSubdomain*.getsilverfin.com/users/auth/openid_connect/callback. Once the OIDC provider is setup, we need the following information to complete the configuration:

- client secret
- client identifier
- host
- token endpoint
- userinfo endpoint
- issuer

[2] http://openid.net/connect/