Introduction

This document describes FLIGHTMAP's identity management options, as is available in FLIGHTMAP release 5 and later. This is the first release to fully implement the FLIGHTMAP Single Sign On (SSO) module that allows FLIGHTMAP connect to external identity providers, for more seamless user experience and more secure identity management in complex IT environments.

Identity management in FLIGHTMAP

FLIGHTMAP has built-in authentication functionality (to identify users) and authorization functionality (to identify each user's access rights to data and functions). This paper describes the authentication. The built-in authentication mechanism is based on identifying each user based on a FLIGHTMAP specific secret username/password combination. The security of this solution depends critically on the security of each user's self-defined password. The policy for password strength (mix of characters, length, absence of patterns), password validity (how much time), and password memory (which old passwords cannot be reused). Imposing a more secure password policy creates more hassle for the users.

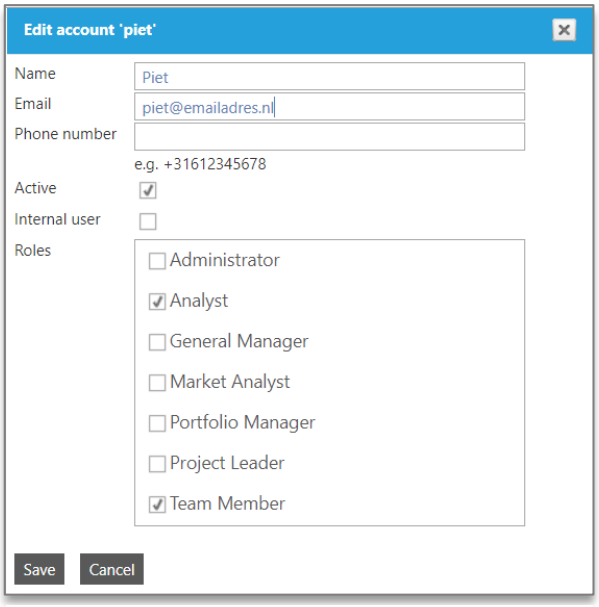

Figure 1 Identity management in FLIGHTMAP

FLIGHTMAP offers a two-factor authentication mechanism that may be activated to keep password strength acceptable to end-users. With this mechanism activated, users identify based on a password and then receive a one-time passcode (OTP) to the cell phone registered as their "second factor" via a text message (SMS). Authentication is only successful when this OTP is also entered correctly.

In addition, FLIGHTMAP access can be restricted to users that (attempt to) log in from their organizations' approved locations such as computers that are in the corporate network, physically or via a Virtual Private Network (VPN). In technical terms, access to the FLIGHTMAP portal can be restricted to limited range of IP addresses.

These settings are part of a standard FLIGHTMAP configuration. However, a serious alternative is to link FLIGHTMAP to a central identity provider, as is available in many organizations.

Single sign on

Single sign-on (SSO) is an identification system that allows an app or website to hand over the verification of users to another party. FLIGHTMAP can for example trust on your Active Directory (via Federation Services ADFS) or Azure system, or on an external provider like OneLogin or iWelcome for user login.

The benefits are obvious:

- Convenience: Users do not have to create and remember a separate set of login credentials for Flightmap.
- Speed: With SSO, users don't have to go through a sign-up and verification processes.
- Control: When users log in on using your own system, you can easily manage access rights and password policies. They will apply automatically for FLIGHTMAP, without FLIGHTMAP requiring identity information. Also, user onboarding and off-boarding are done centrally.

FLIGHTMAP can trust all parties that support the standard communication protocol SAML v2.0. Note FLIGHTMAP depends on the identity provider for authentication (who is this user?). Authorization (access control) for each user is still managed in FLIGHTMAP by means of roles and rights.

SAML-based Single Sign On solution

SAML (Structured Authentication Markup Language) is a standard for SSO. The SAML SSO goal is to minimize the number of times a user needs to login at various web sites. It does this by having the user manually login at only one site, called the identity provider (or IdP). Once the user is logged in on the IdP site, one can automatically get logged in on other sites or apps that trust on the IdP for user verification, without having to provide credentials. These other sites and apps that have a trust relationship with the IdP are called service providers (or SP). FLIGHTMAP SSO is the service provider that can trust on your system as identity provider.

SAML supports two Single sign-on flows: IdP-initiated SSO and SP-initiated SSO. In IdP-initiated SSO, the user starts at the IdP site, logs in and clicks a link to the SP site which initiates SSO. In SP-initiated SSO, the user starts at the SP site and, instead of logging in at the SP site, SSO is initiated via the IdP. FLIGHTMAP supports both, but the common use case is that the user starts FLIGHTMAP in a web browser and gets automatically logged in. This is the SP-initiated SSO flow.

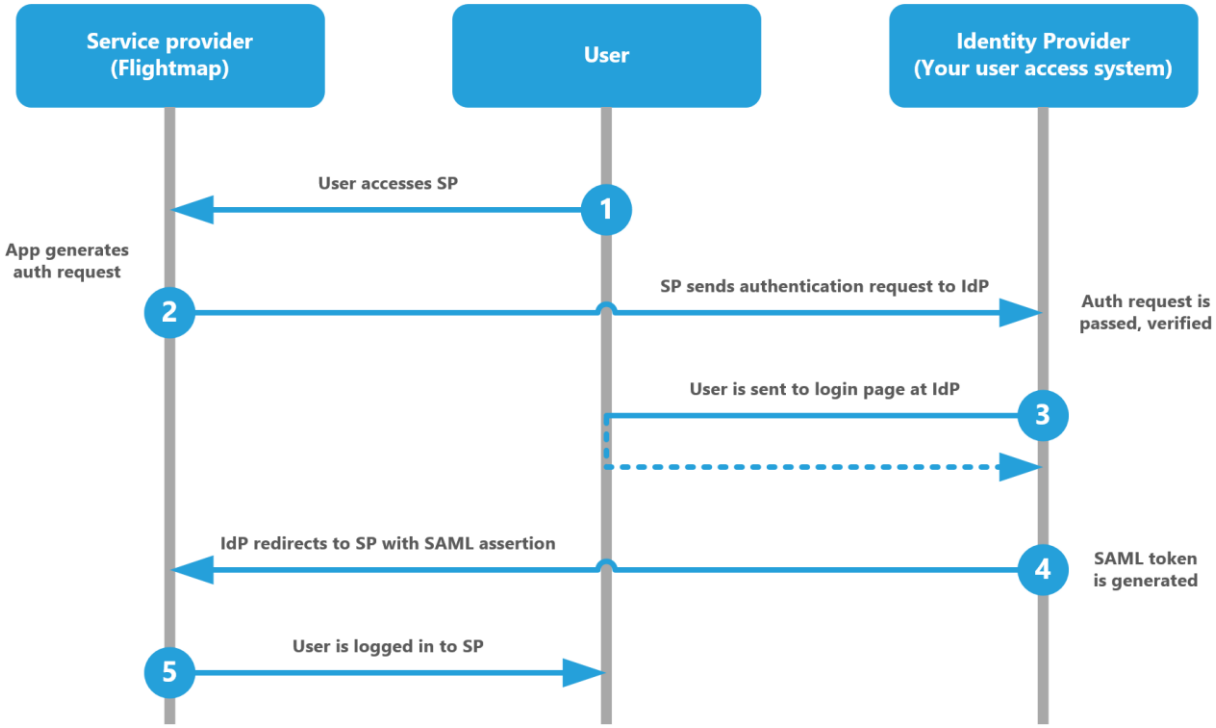

Figure 2 SAML 2.0 Flow

In this flow, the SP sends an XML file to the IdP: a user authentication (verification) request. This request is secured by signing it with a certificate key. Once the identity provider has verified the user and has granted the right to access the service provider, it returns an XML file with user details. This is called a SAML assertion. The SAML assertion should also be encrypted for increased security. If the IdP does not verify the user, the flow will end there. When FLIGHTMAP receives a SAML assertion, it trusts that the user is verified and will grant access depending on the user roles that are defined in the FLIGHTMAP user settings.

For technical details you can refer to the SAML v2.0 specification documents at www.oasisopen.org.

Setting up the Single Sign On for FLIGHTMAP

The SAML protocol requires configuration at both sides.

The IdP needs to configure:

- A user access control system supporting SAML v2.0
- Add FLIGHTMAP as relying party to this system
- A Partner identity provider Url, for example:
  - http://samlsvc.<yourCompany>.com/adfs/services/trust
  - https://app.onelogin.com/saml/metadata/123456
- A Single Sign-on Service Url, like:

  - https://samlsvc.<yourCompany>.com/adfs/ls/ or
  - https://<yourCompany>.onelogin.com/trust/saml2/http-post/sso/123456
- A certificate for encrypting the SAML assertion.

On the FLIGHTMAP side (SP) the following should be configured:

- The Service Provider Url, for example:
  - https://<yourCompany>.flightmap.com
- The Assertion Consumer Service Url (where the IdP sends the assertion to), like:
  - https://<yourCompany>.flightmap.com/AssertionConsumerService.aspx
- A certificate for signing the Authentication request.

Both sides need to share and store these prerequisites.

FLIGHTMAP can support your organization on configuring your user access control system. Detailed step-by-step configuration guidance for various IdP's are available as part of the SSO configuration support package.

Conclusion

FLIGHTMAP offers a range of identity management solutions to make sure users are properly authenticated. The Single Sign On option combines ease of use for end-users with ease of identity on- and off-boarding for the IT function. Since it is based on the proven industry standard SAML 2.0, many different set-ups are supported, and setting it up requires knowledge of this standard.

FLIGHTMAP's SSO requires dedicated configuration as well as an ongoing connection between the FLIGHTMAP infrastructure and the identity provider. The pricing for this is a separate option.

If you are interested, ask for a quotation to support Single Sign On in your FLIGHTMAP portal.

Bicore

Luchthavenweg 18C

5657 EB, Eindhoven, Netherlands

T +31 88 396 2777

info@flightmap.com

www.flightmap.com