eftsure Single Sign On

Introduction

This document outlines the Single Sign On (SSO) integration between eftsure and customers.

Purpose

Allow customers to manage users' access and allow users to log in to eftsure using their network login and password.

Integration

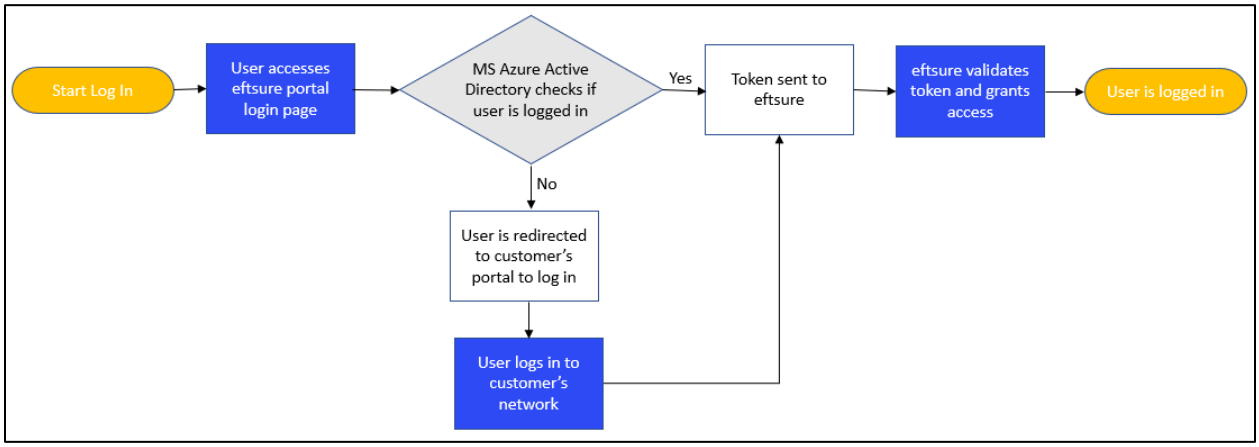
eftsure provides an Azure AD application to facilitate SSO.

Customers restrict access to the eftsure Azure AD application, unless users are granted the relevant permissions to use the application. These access permissions must be configured by customers within their AD domain. The eftsure Azure AD application's client id should be used to create these access permissions.

Independent of users' AD roles, eftsure specific roles can be managed using the eftsure portal by users with an eftsure admin role. eftsure will assign an initial eftsure admin role to a nominated user during the setup process. On first login to eftsure, users will have no eftsure specific roles assigned, and users with the eftsure admin role will need to assign eftsure specific roles to these users.

eftsure will modify the existing log in page to work with SSO integration. This will connect to Customer's Office 365/Microsoft Azure AD to check user is logged in. If not logged in users are redirected to Customer's portal. If the user is logged in a token is provided to eftsure and access is granted.

Process Flow



Notes:

- eftsure to provide the application's client id so customer can setup the relevant access controls
- Customer to provide the tennant id so eftsure knows the request is coming from the customer
- Customer to nominate an initial eftsure admin user. This user must first log in to eftsure and then will be assigned an eftsure admin role by eftsure support. This user will be able to assign the eftsure admin role to other users if required.
- SSO not needed for API
- Use email address as the user name
- Customer to set up an eftsure user within the Customer's environment so eftsure can test the integration