How to integrate Kiuwan with SAML SSO

This guide will show you how to integrate Kiuwan into an SSO-SAML local authentication environment.

Contents:

Introduction

Kiuwan can be integrated with a **Local Authentication** system.

This is a common scenario in organizations that validate their employees' credentials against their authentication system, and do not want them to use other credentials when accessing external services.

If your company uses a corporate authentication service, your users and passwords will most probably be stored in Active Directory, OpenLDAP, IBM Tivoli or a similar system.

If that is your case, it's not needed to have different credentials for your Kiuwan account: you can use the existing ones.

By integrating Kiuwan with your Local Auth service, you will make Kiuwan authentication to delegate on your system, **avoiding the need to use/maintain additional credentials**.

Since the April 2019 release, **Kiuwan allows you to log in to a SAML Single Sign-One (SSO) environment**.

By implementing SSO, a user can log in to different independent systems through the use of a single set of credentials, centrally managed in a repository

Local Authentication scenarios

Depending on your infrastructure, there are at least two possible **scenarios**:

1. **Centralized Authentication**
    a. Do you need to login to every system in your organization using the same user /password? Are you required to type the same credentials to access different systems? This is a clue that your organization maintains a centralized authentication system (i.e. your organization is keeping your credentials in a unique system) that is used by the different systems.
2. **Single Sign-On (SSO)**
    a. Do you only need to authenticate once and you can access the different systems? That is evidence that your systems are internally using an authentication system that is shared by the different applications, making it unnecessary to type your credentials when you access those systems. This is what is called a Single Sign-On environment.

If you want to avoid using/maintaining Kiuwan credentials, determine first which of the above models apply to your organization. Kiuwan supports both models.

There are two different **mechanisms to make Kiuwan work in an SSO environment**.

1. If your organization is using a **centralized credentials repository that does not support SAML** (the most widely adopted SSO standard), you can configure Kiuwan to use it as described in section DelegatedAuthenticationSingleSign-On
2. On the other hand, if your organization is using a **SAML-compliant repository** (e.g. Active Directory FS, Azure AD, CA Single Sign-On, etc), you can configure Kiuwan to use SAML (as described in section SingleSign-on(SSO)withSAML2.0)