

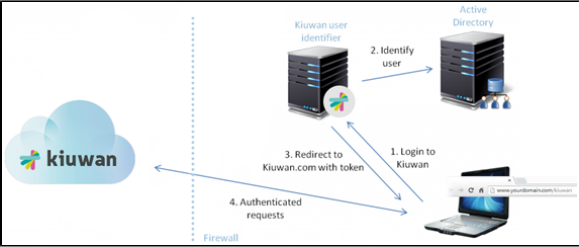
Delegated Authentication Single Sign-On

This page will show you how to set up delegated authentication with Kiuwan.

Centralized authentication is also known as **delegated authentication**.

In this scenario, Kiuwan delegates your authentication to an external system.

The following image describes how it works:

Image	Description
	In this scenario: 1. Login to Kiuwan a. First, you must log in to Kiuwan, but not to www.kiuwan.com. You need to set up a specific URL within your domain. Something similar to http://www.yourdomain.com/kiuwan or http://kiuwan.yourdomain.com 2. Identify user a. That URL will be received by an authentication service application that will delegate your authentication to an external system, e.g. Active Directory, LDAP or a similar system. 3. Redirect to kiuwan.com with a token a. The corporate authentication system checks if you do already have a security context or you need to identify it. If the authentication succeeds, the authentication service application will generate a JWT authentication token including the username (encrypted using a secret key that you can generate in your Kiuwan account settings page). b. Once the auth token is ready, the system redirects to your browser 4. Authenticated request a. The browser requests access to kiuwan.com with an authenticated request that kiuwan.com recognizes, granting access to the requested resource.

You can find a **sample authentication service application** ([kiuwan/kiuwan-local-authentication](#)) as a sample to get started. This sample application uses Tomcat (tomcat-users.xml) as an authentication mechanism, but you can freely adapt to any other external auth system.

You can find details on how to set it up [here](#)