Overview

6.4 Authentication in i2b2 · https://i2b2.org/docs/6-4-authentication-in-i2b2/

Currently there are three methods of authentication supported by the i2b2.

1. Standard i2b2 Authentication

- In this method the i2b2 users are setup in the i2b2 Admin and are stored in the PM Cell.
- The users are authenticated using the PM services.
- Users log into the i2b2 using their i2b2 user id and password.
- Other than setting up your users and projects, this method does not require any additional configuration.

2. Active Directory (AD) Services

- In this method i2b2 users are authenticated using a domain controller in a Windows type of network.
- Users log into the i2b2 using their Windows network id and password.
- Additional parameters are required in order to use this authentication method. See the section titled **Active Directory Authentication** for steps on setting up this method.

3. Lightweight Directory Access Protocol (LDAP)

- In this method i2b2 users are authenticated over an Internet Protocol (IP) network.
- Users log into the i2b2 using the same id and password they currently use to log into other applications in your network.
- Additional parameters are required in order to use this authentication method. See the section titled **LDAP Authentication** for steps on setting up this method.

4. Security Assertion Markup Language (SAML)

- In this method i2b2 users are authenticated against an institutional Identity Provider.

- Users log into the i2b2 by clicking a "Log in with SAML" button and authenticate via their institution's authentication page.
- Additional parameters are required in order to use this authentication method. See the section titled **SAML Authentication** for steps on setting up this method.
- SAML requires other configuration to ensure security. See the **SAML Authentication chapter**.