# Tweezers Identity Module

## Users management

### Users Model

* Username
* Password – stored as hashed + salted.
* Session ID.
* Session ID Expiry date.
* RBAC Role.

### Login API

Will be done based on a username and a password authentication. The API will return a session GUID, This GUID will be at least 128-bit integer.

### Session

Created as the user is successfully authenticated. Revoked after X hours from the last known user interaction.

Note: We would also like to see if there’s an option to revoke the session ID once the user exits the browser.

Note: We would also like to refresh the GUID after each user interaction.

Future: Add CSRF protection.

## RBAC

### Model

* Name
* Permissions:
  + For each Tweezers Discovered entity (or controller), create a permission value.
  + Permission values are:
    - Hide
    - View
    - Edit
  + For example, if the Tweezers app has 3 types of entities, Person, Computer & Cats, the permission table will be:
    - Person: Hide
    - Computer: Edit
    - Cats: View
  + The Tweezers API will enforce the role based on the permission table.

### Predefined Roles

Tweezers will define three predefined roles in advance:

* Administrator: Can edit all entities.
* Viewer: Can only view entities.
* Guest: Can be editable by the admin and will be the default role for guests. By default, will hide everything.