

# TO DO LIST

1  
2  
3



## ToDo & Co

Documentation technique

Guide d'authentification

Frédéric Vanmarcke



VmkDev

17 avril 2022

# Sommaire

<b>Contexte.....</b>	<b>3</b>
<b>Introduction .....</b>	<b>3</b>
<b>Authentification.....</b>	<b>3</b>
Les utilisateurs.....	3
Le système d'authentification .....	4
Les autorisations.....	5
Les rôles .....	5
Les restrictions d'accès .....	5
Annotation @IsGranted.....	6
Voters .....	6
<b>En savoir plus / Documentation : .....</b>	<b>7</b>

## Contexte

Ce guide a pour objectif d'expliciter le **système d'authentification** mis en place pour l'application **ToDo&Co**, afin d'assurer une correcte compréhension par tous les développeurs qui contribueront au développement de l'application, et de définir quels fichiers peuvent être modifiés et comment afin de pallier aux évolutions de l'application. Cette application est accessible par tous, mais son utilisation nécessite d'être enregistré et authentifié.

## Introduction

L'application ToDo&Co est développée sur la base du Framework Symfony qui propose un composant performant permettant de gérer l'authentification des utilisateurs : le composant Security. Ce composant permet d'une part de gérer l'authentification, à savoir d'où proviennent les utilisateurs et comment gérer l'authentification.

D'autre part, ce système permet également de gérer un système d'autorisations, à savoir gérer l'accès à certaines ressources selon le rôle défini de l'utilisateur (visiteur non authentifié, utilisateur authentifié ou encore administrateur).

Ces deux aspects seront traités dans les deux parties suivantes. La majorité des configurations pour ces différents volets sont regroupées au sein du fichier config/packages/security.yaml.

## Authentification

### Les utilisateurs

La configuration des **utilisateurs** est gérée intégralement au sein du fichier **security.yaml**.

- ✓ Un utilisateur est représenté par l'entité **User**, qui implémente la **UserInterface**.
- ✓ La classe User étant une entité Doctrine, les utilisateurs sont stockés en **base de données (bdd)**.

Cette configuration est permise par le paramètre [security.providers](#).

- ✓ L'authentification est réalisée sur la base d'un **nom d'utilisateur (username)**, définie grâce au paramètre **property** et d'un **mot de passe**. Pour des raisons de sécurité évidentes, le mot de passe ne peut être enregistré en clair en bdd. Le paramètre [password hashers](#) permet d'assurer un encodage de ce mot de passe avant enregistrement de l'utilisateur. Dans notre cas, l'utilisation de la clé **auto** pour l'algorithme d'encodage permet à Symfony de sélectionner le meilleur algorithme. Cet **encoder** sera utilisé pour encoder le mot de passe lors de la création d'un utilisateur en bdd, via l'interface [UserPasswordHasherInterface](#).

```
security:
    enable_authenticator_manager: true
    # https://symfony.com/doc/current/security.html#registering-the-user-hashing-passwords
    password_hashers:
        Symfony\Component\Security\Core\User\PasswordAuthenticatedUserInterface: 'auto'
    # https://symfony.com/doc/current/security.html#loading-the-user-the-user-provider
    providers:
        doctrine:
            entity:
                class: App\User
                property: username
```

## Le système d'authentification

Le système d'authentification du composant Security repose sur la définition de **firewalls** qui définissent comment les utilisateurs sont authentifiés, et notamment du **firewall main**.

```
main:
  lazy: true
  pattern: ^/
  form_login:
    login_path: login
    check_path: login
    enable_csrf: true
    always_use_default_target_path: true
    default_target_path: /
  logout:
    path: logout
  switch_user: true
```

- ✓ Le 1er paramètre **lazy** permet d'éviter de créer une nouvelle session s'il n'y a pas besoin d'autorisation particulière, permettant la mise en cache de toutes les URLs ne nécessitant pas d'utilisateur, améliorant ainsi les performances.
- ✓ L'authentification mise en place pour cette application utilise le **provider d'authentification de Symfony** via un formulaire de login (paramètre **form\_login**) dont le nom de route est spécifié par le paramètre **login\_path**. Ce formulaire est protégé par jeton [CSRF](#) grâce au composant Sécurité, dont la vérification est automatiquement réalisée par Symfony. Finalement, le [default\\_target\\_path](#) permet d'indiquer la route que laquelle seront redirigés les utilisateurs après succès de l'authentification. La configuration actuelle utilise les paramètres par défaut du composant Security.
- ✓ Le paramètre **logout** permet de définir le nom de route utilisé pour la déconnexion des utilisateurs. Par défaut les utilisateurs sont redirigés vers la page d'accueil, mais comme celle-ci n'est pas accessible aux utilisateurs non authentifiés, la redirection se fera vers la page de login.
- ✓ Enfin, **switch\_user: true**, donne à certains utilisateurs le super pouvoir de se connecter temporairement en tant que quelqu'un d'autre.

## Les autorisations

Alors que le système d'authentification est quasiment intégralement configuré au sein du fichier **security.yaml**, le système d'autorisations, à savoir la définition de restriction d'accès à certaines ressources en fonction des rôles utilisateurs (ROLE\_USER, ROLE\_ADMIN) peut être réalisée de différentes façons.

### Les rôles

Par l'implémentation de l'interface **UserInterface**, la classe **User** possède une méthode **getRoles()** permettant à Symfony de récupérer lors de la connexion le/les rôle(s) de l'utilisateur, stocké sous forme d'un tableau en base de données.

Les différents rôles définis pour notre application sont les rôles utilisateur (**ROLE\_USER**) et administrateur (**ROLE\_ADMIN**).

Symfony propose également d'autres "statuts" permettant de préciser certains accès : anonyme (**PUBLIC\_ACCESS**) ou encore authentifié (**IS\_AUTHENTICATED\_FULLY**).

```
role_hierarchy:
  ROLE_ADMIN:
    - ROLE_USER
    - ROLE_ALLOWED_TO_SWITCH
```

Une hiérarchie peut être mise en place grâce au paramètre **role\_hierarchy**, spécifiant dans notre cas que le rôle administrateur possède également le rôle utilisateur.

Grace à : [ROLE\\_ALLOWED\\_TO\\_SWITCH](#) et à **switch\_user: true** (dans la configuration main) l'administrateur peut se "connecter" en tant que n'importe qui en ajoutant `?_switch_user=` à l'URL, puis un username.

Pour "sortir" et revenir à l'utilisateur d'origine, ajoutez `?_switch_user=_exit`.

### Les restrictions d'accès

#### *Access control*

Dans le cas de l'application ToDO&Co, une partie des règles de restriction d'accès sont définies dans le fichier **security.yaml** sous le paramètre **access\_control**. Les règles décrites ci-dessous définissent les comportements suivants :

- ✓ L'url `"/login`" est accessibles aux utilisateurs non authentifiés.
- ✓ Toutes les URLs commençant par `"/users`" ne sont accessibles qu'aux utilisateurs ayant le rôle administrateur.
- ✓ L'ensemble des autres URLs est accessible aux utilisateurs authentifiés ayant le rôle utilisateur.

```
# Easy way to control access for large sections of your site
# Note: Only the *first* access control that matches will be used PUBLIC_ACCESS
access_control:
  - { path: ^/login, roles: PUBLIC_ACCESS }
  - { path: ^/users, roles: ROLE_ADMIN }
  - { path: ^/, roles: ROLE_USER }
```

## Annotation @IsGranted

Comme nous l'avons évoqué précédemment, toutes les routes liées à la gestion des utilisateurs possédant une URL commençant par "/users/" ne sont accessibles qu'aux utilisateurs ayant le rôle administrateur.

Cette configuration au sein du fichier **security.yaml** aurait également pu être mise en place au sein des contrôleurs grâce à l'annotation **IsGranted('ROLE\_ADMIN')** du Sensio/FrameworkExtraBundle (Sensio\Bundle\FrameworkExtraBundle\Configuration\IsGranted), soit directement au niveau des annotations globales de la classe **UserController**, soit au niveau des annotations des différentes méthodes dont on veut restreindre l'accès. Si certaines pages liées aux utilisateurs devaient devenir accessibles non plus aux seuls administrateurs, cette méthode serait plus adaptée à mettre en place.

Cette annotation est également prise en charge au sein des templates par le moteur de templating Twig, et a été mis en place notamment pour que les boutons de gestion des utilisateurs ("Créer un utilisateur", "Voir les utilisateurs") ne soient visibles et accessibles uniquement par les personnes possédant le rôle administrateur.

```
<!-- Page Content -->
<div class="container">
  <div class="row row-button">
    {% if is_granted("ROLE_ADMIN") %}
      <a href="{{ path('user_create') }}" class="btn btn-primary">Créer un utilisateur</a>
      <a href="{{ path('user_list') }}" class="btn btn-primary">Voir les utilisateurs</a>
    {% endif %}

    {% if app.user %}
      <a href="{{ path('logout') }}" class="pull-right btn btn-danger">Se déconnecter</a>
    {% endif %}

    {% if not app.user and 'login' != app.request.attributes.get('_route') %}
      <a href="{{ path('login') }}" class="btn btn-success">Se connecter</a>
    {% endif %}
  </div>
```

## Voters

Finalement, le 3e système proposé par le composant Security pour gérer les restrictions d'accès est le système de **Voters**, dont l'implémentation se fait au niveau des Controller. Ce système a été mis en place pour restreindre la possibilité de supprimer une tâche à l'auteur de la tâche, et pour les tâches liées à "l'utilisateur anonyme", de restreindre leur suppression aux administrateurs.

Les Voters sont le moyen le plus puissant de Symfony pour gérer les autorisations. Ils vous permettent de centraliser toute la logique d'autorisation, puis de les réutiliser à de nombreux endroits.

```
#[Route('/tasks/{id}/delete', name: 'task_delete')]
#[IsGranted('TASK_DELETE', subject: 'task', statusCode: 401)]
public function deleteTaskAction(Task $task): Response
{
    $this->taskManager->manageDeleteAction($task);
    $this->addFlash('success', 'La tâche a bien été supprimée.');
```

*(Note: The original image contains a redacted line of code, likely a return statement, which has been omitted for brevity and to match the visible content.)*

```
    return $this->redirectToRoute('task_todo_list');
}
```











Pour ce faire, une classe **TaskAccessVoter** a été créée et implémente l'interface **VoterInterface**. Cette classe a pour objectif d'autoriser la suppression de la tâche seulement si :

- ✓ L'utilisateur authentifié est administrateur et que la tâche en question est liée à un utilisateur "anonyme".
- ✓ L'utilisateur authentifié est bien l'auteur de la tâche.

```
/**
 * @param Task $task contains task information
 * @param User $user contains user information
 */
private function canDelete(Task $task, User $user): bool
{
    if ($this->security->isGranted('ROLE_ADMIN') && (null === $task->getAuthor())) {
        return true;
    }

    return $user === $task->getAuthor();
}
```

## En savoir plus / Documentation :

-  [Security](#)
-  [Authentication](#)
-  [Authorization](#)
-  [Loading the User: The User Provider](#)
-  [Hashing the Password](#)
-  [CSRF Protection in Login Forms](#)
-  [Changing the default Page](#)
-  [Creating a Custom User Checker](#)
-  [How to Impersonate a User](#)
-  [ROLE\\_ALLOWED\\_TO\\_SWITCH](#)
-  [@Security & @IsGranted](#)
-  [How to Use Voters to Check User Permissions](#)