Documentation administrateur

Introduction

Esup-signature propose une interface d'administration qui permet le suivi des demandes en cours, le paramétrage des circuits de signatures ou des formulaires, ainsi que divers outils qui seront détaillés après.

La configuration générale de l'application se fait via le fichier de configuration application.yml avant la compilation du projet voir : Configuration

Enfin pour des besoins très précis il est possible d'écrire directement des classes spécifiques pour gérer les sources de données, le pré-remplissage des formulaires ou encore pour décrire des circuits de signatures.

Pour avoir accès à l'espace "Admin" l'utilisateur doit disposer du rôle ROLE_ADMIN tel que défini dans la propriété group-mapping-role-admin: d u fichier de configuration voir : Configuration securité

Liste des demandes

La vue demande est la première vue accessible lorsque que l'on clique sur "Admin" dans la barre de navigation (ou sur la couronne)

Elle permet à l'administrateur de consulter toutes les demandes. Les demandes peuvent être filtrées en fonction de leur statut

Pour autant, l'administrateur ne peut pas consulter les documents, il peut simplement vérifier la liste des événements et si besoin supprimer les demandes.

Les circuits

Voir la page dédiée aux circuits : Gestion des circuits

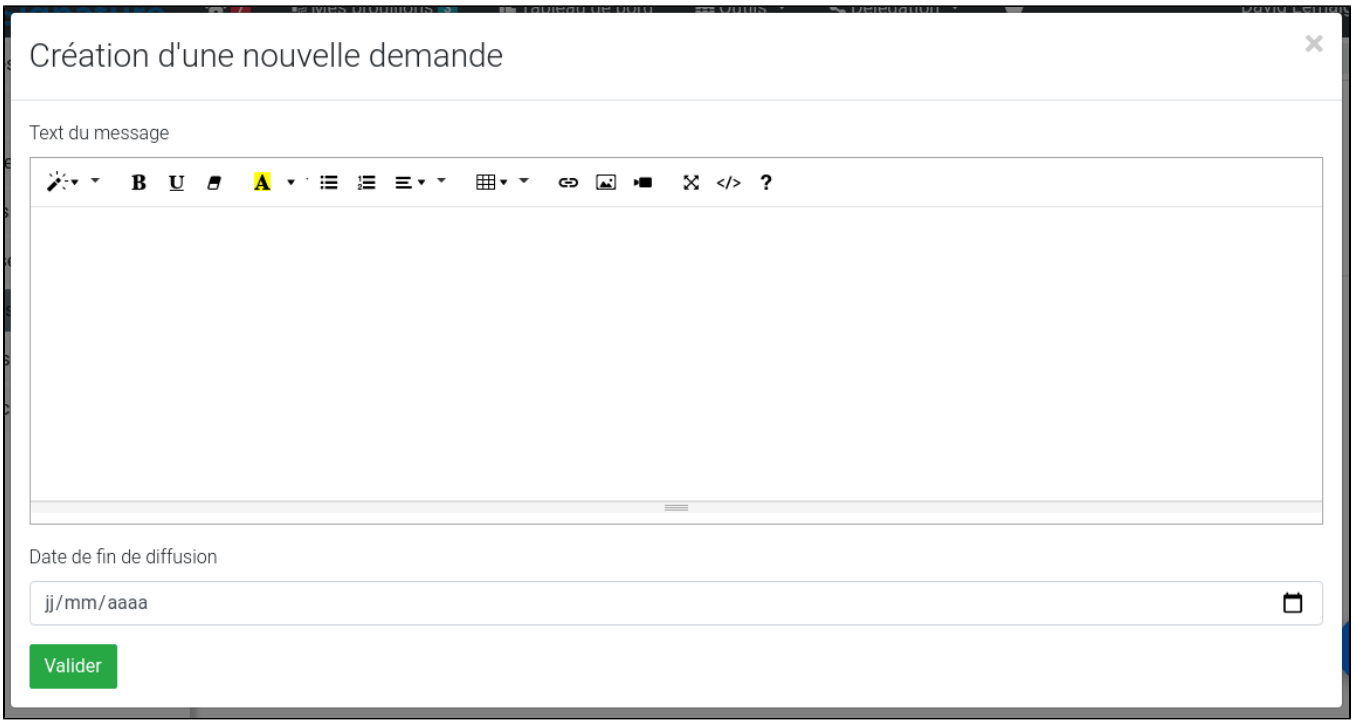
Les formulaires

Voir la page dédiée aux formulaires : Gestion des formulaires

---

Les messages d'information

Esup-signature propose un système permettant transmettre des messages d'information à tous les utilisateurs. Pour cela, il faut se rendre sur "Admin", "Messages" puis cliquer sur le bouton bleu "+"



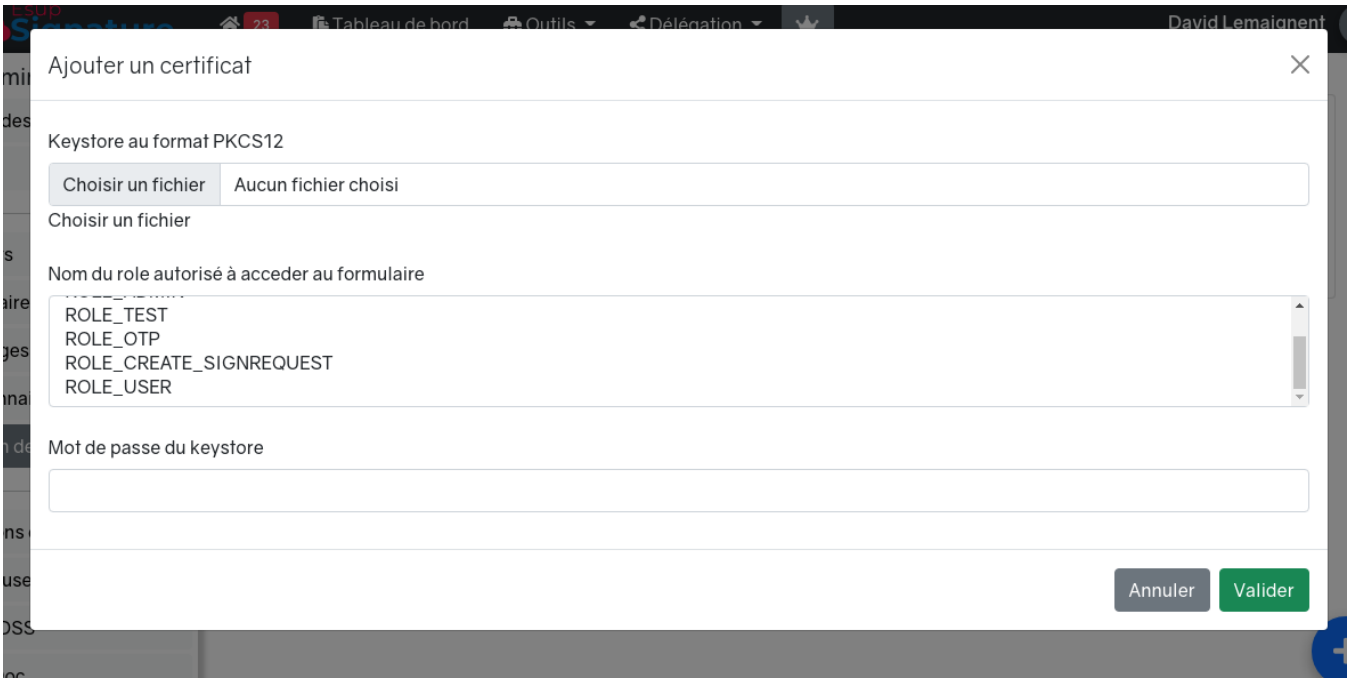
Vous pouvez alors saisir un message ainsi qu'une date de fin de diffusion. Tous les utilisateurs verront ce message et auront la possibilité de le désactiver une fois consulté.

Gestion des certificats

Esup-signature propose aux administrateurs la possibilité de partager des certificats "établissement" pour une certaine population (en fonction des rôles des utilisateurs).

L'objectif est de permettre aux utilisateurs de signer électroniquement (avec un certificat donc) sans avoir l'obligation d'avoir un certificat à leur nom dans leur profil esup-signature.

Au moment de la signature, les utilisateurs concernés se verront proposer le certificat correspondant à leur rôle (en plus de leur éventuel certificat personnel).



Pour ajouter un certificat, il faut se rendre dans Admin Gestion des certificats. Puis lors de l'ajout, choisir le keystore contenant le certificat (PKCS12), choisir les rôles autorisés à l'utiliser et enfin saisir le mot de passe du keystore.

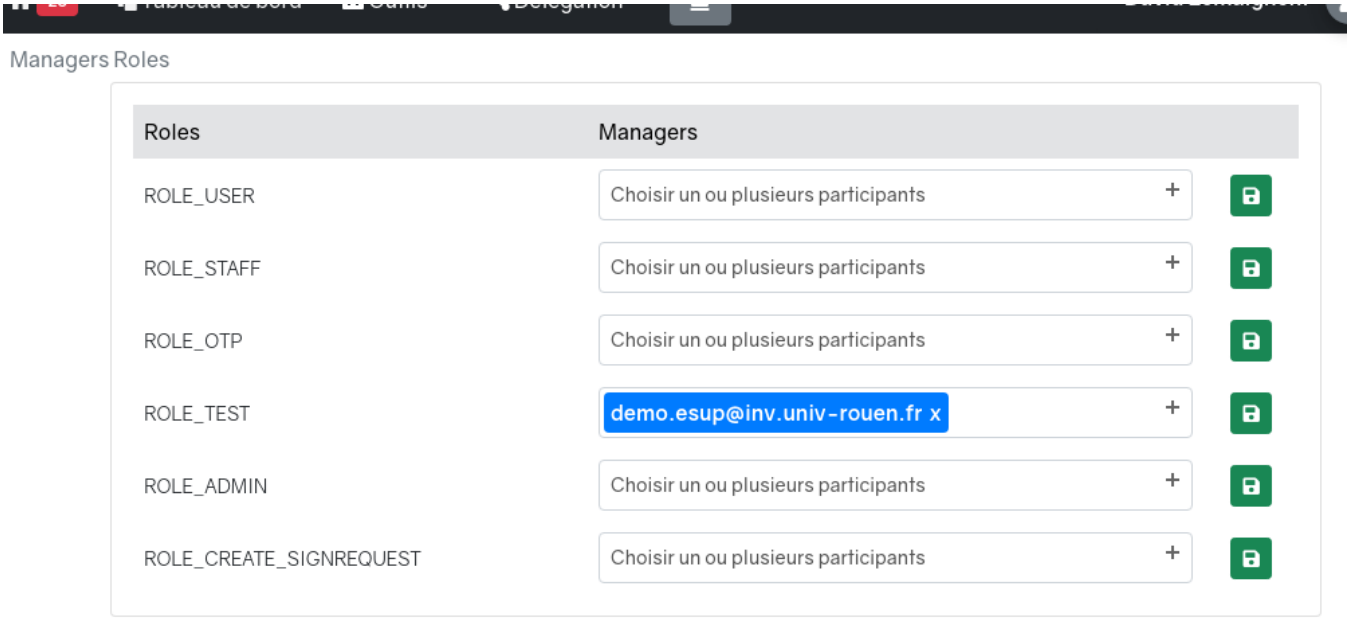
⚠ Les utilisateurs non pas de mot de passe à saisir lors de la signature

---

Gestionnaires des rôles

Depuis la version 1.13, il est possible de déclarer des gestionnaires de rôles. Cela a pour but de permettre à des utilisateurs de créer des circuits et des formulaires à destination des personnes possédants le rôle concerné.

Pour chaque rôle connu dans esup-signature, il est possible d'affecter une ou plusieurs personnes :



⚠ Dans esup-signature, il y a deux façons d'obtenir des rôles:

- à l'aide de filtre LDAP si votre environnement le permet voir :Configuration#ldap.1
- en possédant un groupe dans vos attributs de session dont le prefix correspond à celui configuré dans **group-to-role-filter-pattern**, voir : Configuration#security
- à l'aide **group-mapping-spel** qui permet de définir les règles d'attribution de groupes, voir : Configuration#security

Pour accéder à l'application il faut impérativement avoir le rôle : ROLE_USER. Pour la partie administration, il faut ROLE_ADMIN

Les rôles obtenus seront copiés dans le profil de l'utilisateur. Un utilisateur peut obtenir des rôles du type : staff, student, test, ordre_de_mission, marches, etc.... ceci grâce à des groupes correspondant au pattern **group-to-role-filter-pattern** (le texte qui suit le préfixe est converti en rôle ex : ROLE_ORDRE_DE_MISSION) ou à l'aide de **mapping-groups-roles**

Les rôle autres (que user et admin) peuvent être utilisés lorsque vous configurez un formulaire ou un circuit pour y restreindre les accès.

Pour une explication détaillée du fonctionnement de la sécurité, voir : Configuration de la sécurité

Switch user

Le switch user permet à l'administrateur de prendre la place d'un autre utilisateur. Cela peut être utile pour reproduire ou constater un problème spécifique à un utilisateur. Toutefois, pour des raisons de confidentialité, cette option n'est pas active par défaut. Pour débloquer cette fonctionnalité il faut modifier le fichier application.yml et mettre la valeur enable-su à true