



Création d'un serveur Passbolt

Création d'un serveur Passbolt Production – 1.0 Date 05/02/26

Type	Date	Version	Intervenant
Création	05/02/26	1.0	Luka.E



Table des matières :

Prérequis	3
1. Ajout des dépôts Passbolt et paramétrage proxy	
1.1 Ajout des dépôts requis	4
1.2 Configuration du proxy	6
2. Installation des paquets Passbolt	7
3. Installation du serveur Passbolt	
3.1 Création de la base de données	8
3.2 Configuration du service WEB (Nginx)	11
4. Configuration du Passbolt	12
5. Connexion au compte Admin	26
6. Configuration de l'inscription mail	31
7. Difficultés rencontrées	
7.1 Problème de nom de domaine	33
7.2 Certificats SSL non reconnus	34



Prérequis

Afin de pouvoir correctement installer ce serveur, voici les prérequis à avoir :

- Une machine virtuelle avec Debian 13 Server installée dessus (un serveur physique fonctionne aussi)
- Plusieurs paquets de base (Nano, Curl, etc...)
- Certificat WEB HTTPS ainsi que sa clé

*** Pour des raisons de confidentialité, certaines parties des captures d'écrans seront masquées. ***



1. Ajout des dépôts Passbolt et configuration Proxy

Rappel : Cette étape est nécessaire en raison du proxy venant gérer les sites WEB ainsi que les téléchargements depuis ces derniers. Si vous n'êtes pas bloqué par un proxy, vous pouvez directement passer à la 2e partie.

1.1 Ajout des dépôts requis

Étape 1 : Accéder à la liste des sources avec la commande suivante : `sudo nano /etc/apt/sources.list`

```
GNU nano 8.4 /etc/apt/sources.list *
deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie contrib main non-free non-free-firmware
deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-updates contrib main non-free non-free-firmware
deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-proposed-updates contrib main non-free non-free-firmware
deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-backports-sloppy contrib main non-free non-free-firmware
deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-backports contrib main non-free non-free-firmware
```

° Les sources actuelles sont celles de l'intranet

Étape 2 : Désactiver les dépôts actuels en ajoutant un « # » devant chacun d'entre eux (ils deviendront de simples commentaires).

```
#deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie contrib main non-free non-free-firmware
#deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-updates contrib main non-free non-free-firmware
#deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-proposed-updates contrib main non-free non-free-firmware
#deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-backports-sloppy contrib main non-free non-free-firmware
#deb [trusted=yes] http://mirror.intranet.quebec.ca/debian trixie-backports contrib main non-free non-free-firmware
```



Étape 3 : Ajouter les dépôts requis.

```
GNU nano 8.4 /etc/apt/sources.list
deb [trusted=yes] http://deb.debian.org/debian trixie contrib main non-free non-free-firmware
#deb [trusted=yes] http://deb.debian.org/debian trixie-updates contrib main non-free non-free-firmware
#deb [trusted=yes] http://deb.debian.org/debian trixie-proposed-updates contrib main non-free non-free-firmware
#deb [trusted=yes] http://deb.debian.org/debian trixie-backports-sloppy contrib main non-free non-free-firmware
#deb [trusted=yes] http://deb.debian.org/debian trixie-backports contrib main non-free non-free-firmware
deb [trusted=yes] https://download.passbolt.com/ce/debian buster stable
deb [trusted=yes] http://deb.debian.org/debian trixie main non-free-firmware
deb [trusted=yes] http://deb.debian.org/debian trixie-updates main non-free-firmware
deb-src [trusted=yes] http://deb.debian.org/debian trixie main non-free-firmware
deb-src [trusted=yes] http://deb.debian.org/debian trixie-updates main non-free-firmware
```

- ° Celle entourée en rouge est le dépôt Passbolt (Community Edition) pour Debian
- ° Celles entourées en vert sont les dépôts de base de Debian (nécessaires pour installer certains paquets et updates)

Étape 4 : Sauvegarder la modification avec Ctrl + X et confirmer avec « Y » ou « O ».



1.2 Paramétrage proxy

Étape 1 : Accéder au fichier « apt.conf » à l'aide de la commande :
`sudo nano /etc/apt/apt.conf`, un fichier vide s'ouvrira.



Étape 2 : Ajouter l'utilisateur, le MDP ainsi que l'IP du proxy et son port.



`http://user:mdp@adresse.ip:port` ← à renseigner entre les guillemets

Étape 3 : Sauvegarder la modification avec `Ctrl + X` et confirmer avec « Y » ou « O ».

Si vous souhaitez vérifier si les paquets sont bien accessibles, il suffit d'utiliser la commande `sudo apt update`, et nous verrons les sources récupérer des mises à jour.



2. Installation des paquets Passbolt

Étape 1 : Télécharger les dépendances Passbolt avec cette commande :

Utilisation de l'utilisateur
du proxy

```
curl -x "http://user:mdp@adresse.ip:port" -LO  
"https://download.passbolt.com/ce/installer/passbolt-repo-setup.ce.sh" --insecure
```

```
  Total    Received  Xferd Average Speed  Time   Time   Time Current  
                Dload Upload Total   Spent  Left  Speed  
100 10130 100 10130    0    0 56272    0 --:--:-- --:--:-- --:--:-- 56592  
root@      :/home/admin-dsisi#
```

Le paquet a bien été installé

Étape 2 : Télécharger le fichier SHA512SUM (ce script sera nécessaire pour l'installation du Passbolt) :

```
curl -x "http://user:mdp@adresse.ip:port" -LO https://github.com/passbolt/passbolt-dep-  
scripts/releases/latest/download/passbolt-ce-SHA512SUM.txt
```



3. Installation du Passbolt

Maintenant que les paquets ont bien été installés, nous allons pouvoir lancer la création du serveur.

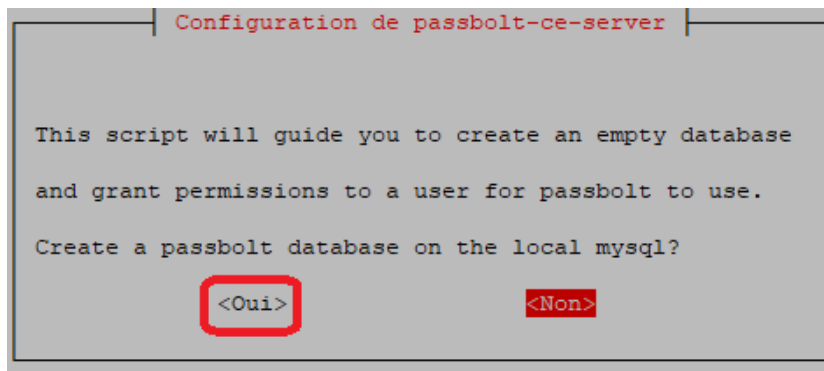
3.1 Création de la base de données

Étape 1 : Lancer l'installation avec le script

```
sudo apt install pasbolt-ce-server
```

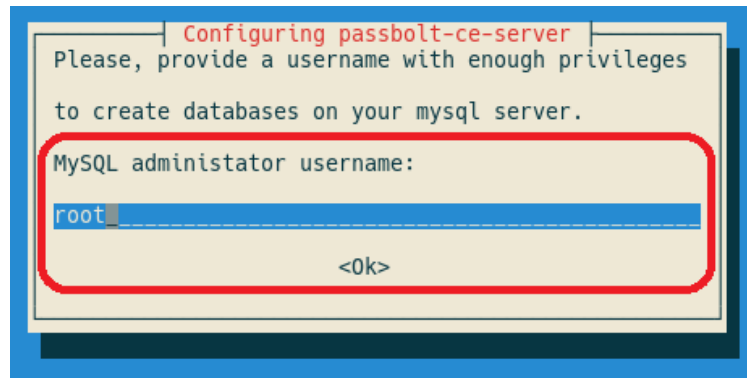
Une fenêtre apparaît :

Le configurateur nous dit que ce script va créer une base de données vide. Étant donné que nous n'en avons pas, nous allons choisir « **Oui** ».

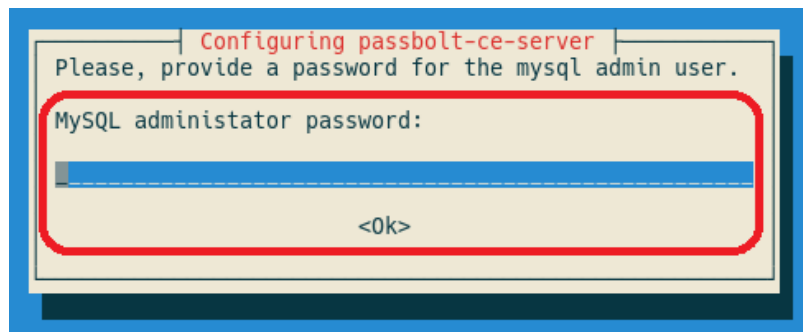




Étape 2 : Renseigner le nom du compte administrateur de MariaDB.

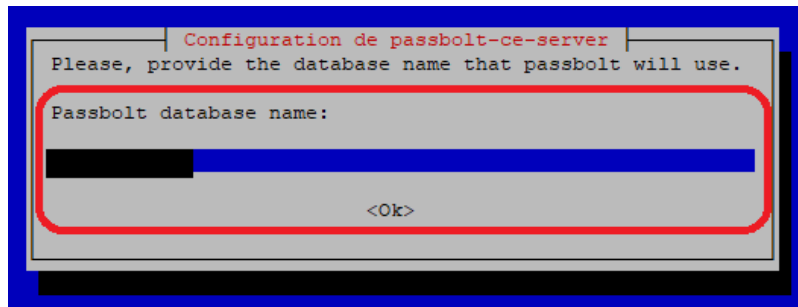


Étape 3 : Renseigner le MDP root.

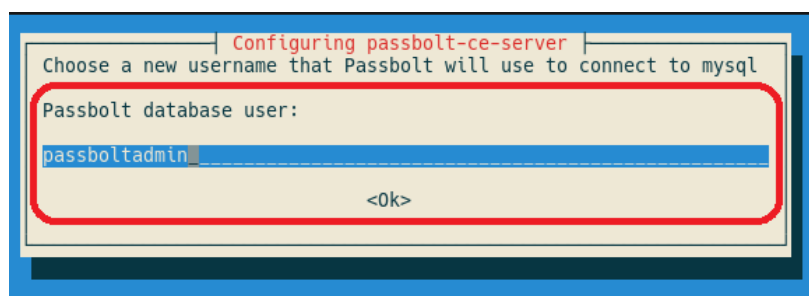




Étape 4 : Choisir un nom pour la BDD.

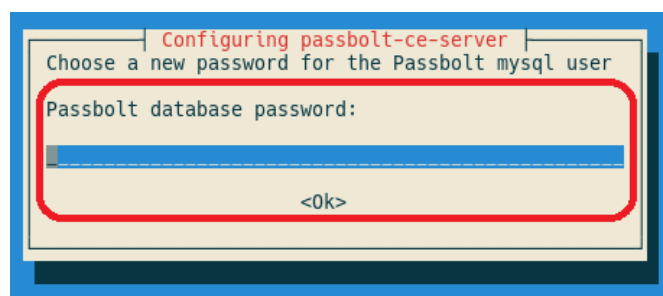


Étape 5 : Renseigner un nouvel utilisateur cette pour cette BDD.



Note : la BDD a dû être refaite durant l'installation. L'utilisateur est donc « admin-dsisi ».

Étape 6 : Renseigner le MDP de l'utilisateur.

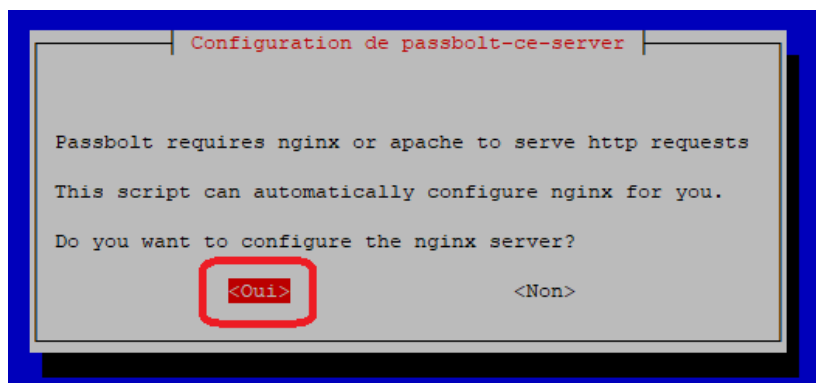




3.2 Configuration du service WEB (Nginx)

Lors de cette configuration du serveur WEB, ce Passbolt devra être accessible depuis le port HTTPS (443).

Étape 1 : Le configurateur va vous demander de configurer Nginx pour nous, choisir « **oui** »





Étape 2 : Cette étape demande une configuration SSL pour le site Passbolt créé par Nginx :

- « None » : Qui retire le protocole SSL et donc la connexion au site ne sera pas cryptée.
- « Manual » : Cette option demandera de renseigner un certificat ainsi qu'une clé spécifique (notamment des certificats provenant d'autorités dans l'organisation)
- « Automatic » : Génère un certificat et une clé automatique pour ce domaine.

```
Configuration de passbolt-ce-server
This script adds a nginx site for passbolt. Select which SSL setup for the nginx config:
"none" will delay SSL configuration to a later stage.
"manual" allows you to provide the SSL keys.
"auto" will generate SSL keys for your domain through Letsencrypt.org
Passbolt nginx setup:
  none
  manual
  auto
  <Ok>
```

Dans ce cas de figure précis, choisir « Manual », puis confirmer avec « OK ».



Étape 3 : Renseigner le nom de domaine.

Configuration de passbolt-ce-server

Provide the domain name where you will run Passbolt.
If you do not have a domain name or you are not sure, introduce the ip address of this machine.

Passbolt domain name:
passbolt.sgami

<Ok>

Étape 4 : Renseigner l'emplacement du certificat.

Configuration de passbolt-ce-server

This is the path where you have your SSL certificate stored.
If you have not uploaded your SSL certificate to this machine, do it now.

Provide the filename for the SSL fullchain key:

<Ok>

Ex de chemin : /home/user/cert.pem (le chemin dépend d'où le certificat a été mis par l'utilisateur)

Étape 5 : Renseigner l'emplacement

Configuration de passbolt-ce-server

If you have not uploaded your SSL key to this machine, do it now.

Provide the filename for the SSL Private Key:
/home/admin-dsisi/key.pem

<Ok>



Le script termine son installation.

```
root@S :/home/admin-dsisi# sudo apt install passbolt-ce-server
Installation de :
  passbolt-ce-server

Paquets suggérés :
  python-certbot-nginx | python-certbot-apache

Sommaire :
  Mise à niveau de : 0. Installation de : 1Supprimé : 0. Non mis à jour : 0
  Taille du téléchargement : 0 B / 13,3 MB
  Espace nécessaire : 57,6 MB / 233 GB disponible

Préconfiguration des paquets...
Sélection du paquet passbolt-ce-server précédemment désélectionné.
(Lecture de la base de données... 47370 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ../passbolt-ce-server_5.8.0-1_all.deb ...
Dépaquetage de passbolt-ce-server (5.8.0-1) ...
Progression : [ 20% ]
```

Une fois le script terminé, ce message apparaîtra avec le lien pour s'y connecter.

```

Passbolt
Open source password manager for teams
-----
A JWT key pair was successfully created.
Public key path: /etc/passbolt/jwt/jwt.pem
Secret key path: /etc/passbolt/jwt/jwt.key
-----
Well done! Visit https://passbolt.sgami.zonenord.minint.fr to finish installation
-----
Traitement des actions différées (« triggers ») pour nginx (1.26.3-3+deb13ul) ...
Triggering nginx reload ...
root@S :/home/admin-dsisi#
```



Afin de vérifier si la BDD ainsi que le serveur WEB sont bien installés, plusieurs commandes peuvent être effectuées :

- sudo systemctl status mariadb (MariaDB étant le système de BDD) :

MariaDB est actif

```
root@passbolt:/home/admin-dsisi# sudo systemctl status mariadb
● mariadb.service - MariaDB 11.8.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Wed 2026-02-04 12:22:40 CET; 1 day 22h ago
     Invocation: 9339ddb994bc4fafa915f34408cac645
       Docs: man:mariadb(8)
             https://mariadb.com/kb/en/library/systemd/
   Process: 803 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
   Process: 813 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/usr/bin/galera_recovery"; [ $? -eq 0 ]
   Process: 920 ExecStartPost=/bin/rm -f /run/mysql/wsrep-start-position (code=exited, status=0/SUCCESS)
   Process: 922 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 844 (mariadb)
    Status: "Taking your SQL requests now..."
     Tasks: 12 (limit: 126301)
    Memory: 201M (peak: 201.6M)
       CPU: 1min 5.558s
    CGroup: /system.slice/mariadb.service
           └─844 /usr/sbin/mariadb
```

- sudo systemctl status nginx (Service WEB)

Nginx est actif

```
root@passbolt:/home/admin-dsisi# sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Wed 2026-02-04 12:22:37 CET; 1 day 22h ago
     Invocation: 0c69672343e84397a24a084af917f01d
       Docs: man:nginx(8)
   Process: 804 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Process: 838 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Main PID: 846 (nginx)
     Tasks: 5 (limit: 19136)
    Memory: 16.6M (peak: 19.1M)
       CPU: 13.206s
    CGroup: /system.slice/nginx.service
           └─846 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─847 "nginx: worker process"
               └─848 "nginx: worker process"
                 └─850 "nginx: worker process"
                   └─851 "nginx: worker process"
```



Afin de voir si la BDD ainsi que l'utilisateur ont bien été créés, se connecter à la console d'administration de MariaDB :

```
sudo mysql -u root -p
```

Puis, renseigner le MDP du compte root.

```
root@passbolt:/home/admin-dsisi# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9126
Server version: 11.8.3-MariaDB-0+deb13ul from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Une fois arrivé sur le terminal MariaDB, taper la commande show databases;

```
MariaDB [(none)]> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| mysql                   |
| passboltdb             |
| performance_schema     |
| sys                     |
+-----+
5 rows in set (0,001 sec)
```

La BDD du serveur Passbolt est bien visible.



SELECT user FROM mysql.user; sert à lister les utilisateurs.

```
MariaDB [(none)]> SELECT user FROM mysql.user;
+-----+
| User          |
+-----+
| admin-dsisi   |
| mariadb.sys   |
| mysql         |
| root          |
+-----+
4 rows in set (0,001 sec)
```

Les comptes « root » et « admin-dsisi » (l'utilisateur du Passbolt) sont également visibles.

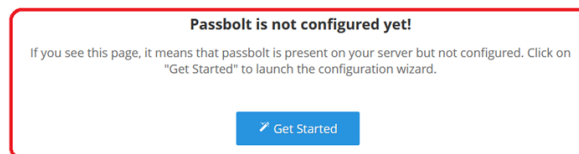


4. Configuration du Passbolt

Étape 1 : Connexion au Passbolt via son lien.



Une fois connecté, cette page s'affichera afin de dire que le Passbolt doit être configuré.



Cliquer sur « Get Started ».



Étape 2 : Vérification de l'environnement

The screenshot shows the Passbolt configuration interface. At the top, there is a header with the Passbolt logo and the text "Welcome to Passbolt! Let's get started with the configuration." Below this, a sidebar on the left lists the configuration steps: 1. System check, 2. Database, 3. Server keys, 4. Options, 5. Emails, 6. First user, 7. Installation, and 8. That's it! The main content area displays a success message: "Nice one! Your environment is ready for passbolt." Below this message are three green bars indicating successful checks: "Environment is configured correctly.", "GPG is configured correctly.", and "SSL access is enabled." A blue button labeled "Start configuration" is positioned at the bottom of this section. To the right, there is a "Help" section with the text "Need help? You can find more information on how to install passbolt in the official online help." and a "Help" button.

L'environnement est prêt à accueillir le Passbolt ainsi que ces futurs fichiers.



Étape 3 : Configurer de la BDD.

Plusieurs points sont à souligner :

1 – L'url de la BDD doit être l'ip « 127.0.0.1 » (adresse localhost) car la base ainsi que le Passbolt sont sur une même machine.

Si la BDD est sur une machine séparée du Passbolt, configurer MariaDB en conséquence puis mettre l'ip de la machine BDD. Enfin, laisser le port sur 3306 qui est le port de MariaDB.

2 – L'utilisateur est le MDP à renseigner sont ceux qui ont été créés lors de la création de la BDD.

3 – Idem pour la BDD.

Database configuration

Database connection url *		
mysql:// ▾	127.0.0.1	3306 ▾
Username *	Password *	
admin-dsisi	●●●●●●●●●●●●●●●●●●●●	
Database name *		
passboltdb		



Étape 4 : Renseigner le nom du serveur ainsi que de son adresse mail attitrée.

Create a new OpenPGP key for your server

Server Name *
passbolt.sgam [REDACTED]

Server Email *
[REDACTED]

Comment
add a comment (optional)



Étape 5 : Renseigner les paramètres SMTP.

- 1 – Choisir le nom d'envoi
- 2 – Choisir l'adresse mail du Passbolt
- 3 – Renseigner l'adresse du serveur STP
- 4 – Choisir « No » pour l'utilisation du TLS pour les mails
- 5 – Renseigner le port SMTP
- 6 – Choisir utilisateur et MDP en méthode d'authentification

passbolt Enter your SMTP server settings.

- 1. System check
- 2. Database
- 3. Server keys
- 4. Options
- 5. Emails**
- 6. First user
- 7. Installation
- 8. That's it!

Sender name *
sgami-nord-noreply **1**

Sender email *
sgami-nord-noreply@interieur.gouv.fr **2**

SMTP server configuration

SMTP host *
[redacted] **3**

Use TLS? *
No **4**

Port *
25 **5**

Authentication method *
Username & password **6**

Username
username

Password
password

Laisser ces 2 zones vides.



Étape 6 : Envoyer un mail de test afin de voir si SMTP est bien paramétré.

Why do I need a SMTP server?

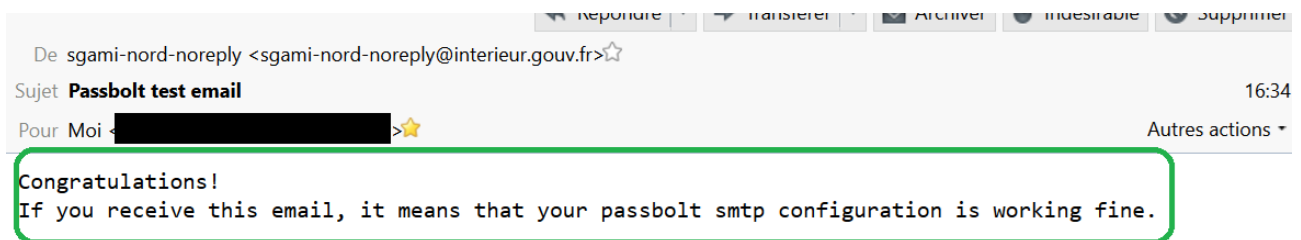
Passbolt needs an smtp server in order to send Invitation emails after an account creation and to send email notifications.

Send test email

Test your configuration by sending a test email.

The test email has been sent successfully!

Send test email



Le mail de test a bien été envoyé.



Étape 7 : Ne rien changer sur cette page.

Options

Full base url *

This is the url where passbolt will be accessible. This url will be used for places where the passbolt url cannot be guessed automatically, such as links in emails. No trailing slash.

Force SSL? *

Forcing SSL means that passbolt will not accept connections coming from a non secure protocol. If SSL is forced, your server has to be configured for HTTPS. It is highly recommended that you do so.



Étape 8 : Renseigner les informations nécessaires pour le premier utilisateur.

passbolt → **Create your user account!**

1. System check
2. Database
3. Server keys
4. Options
5. Emails
- 6. First user**
7. Installation
8. That's it!

Admin user details

First name *

Last name *

Username *

[Next](#)

Note : L'username est en réalité de l'email du compte.

Étape 9 : Finalisation de l'installation

Installing

Passwords so secret, even we didn't know we had them.



5. Connexion au compte Admin

Une fois que la configuration est faite, la page va se rafraîchir d'elle-même. Nous allons donc pouvoir nous connecter au Passbolt avec notre compte Admin.

Étape 1 : Installer l'extension Passbolt sur le navigateur.



Puis cliquer sur « **Ajouter à Firefox** »

▲ La sécurité de ce module n'est pas contrôlée par Mozilla. Assurez-vous de sa fiabilité avant de l'installer. [En savoir plus](#)

 **Passbolt - Open source password manager for teams** [Ajouter à Firefox](#)
par **passbolt**

Passbolt is an open source password manager designed for collaboration. Securely create, manage and monitor your passwords. Share them instantly with your team.

★ 4.4 (58 critiques)  31 961 utilisateurs-trices



❖ Ajouter Passbolt - Open source password manager ? Cette extension aura l'autorisation de :

- Accéder à vos données pour tous les sites web
- Ajouter des données dans le presse-papiers
- Accéder aux onglets du navigateur

[En savoir plus](#)

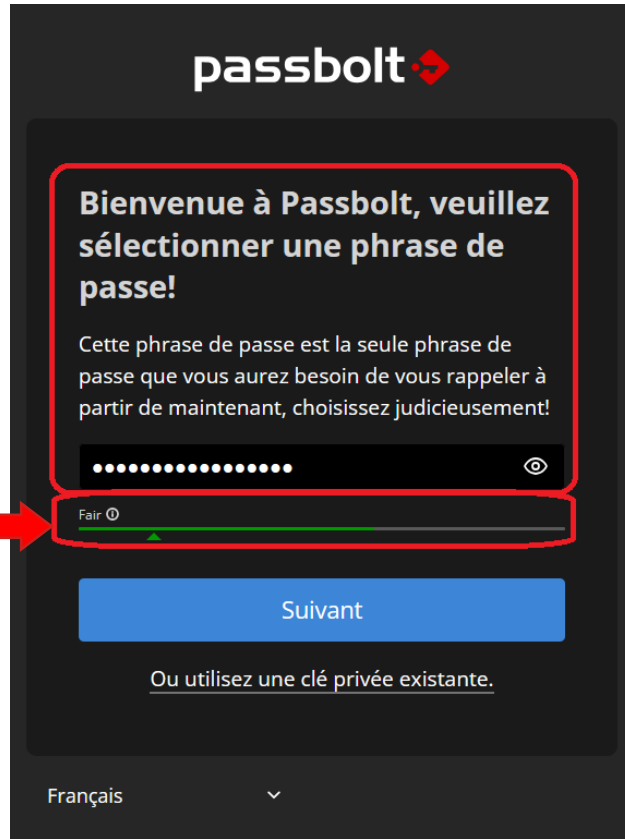
Confirmer l'ajout

Il faudra également autoriser en navigation privée.

Autoriser cette extension à s'exécuter dans une fenêtre de navigation privée

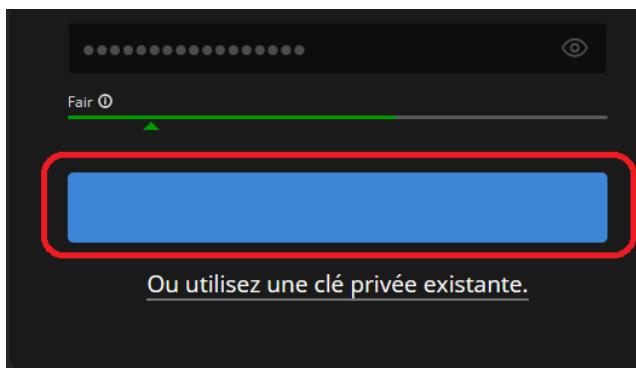


Étape 2 : Créer une phrase de passe.



La résistance du MDP doit être au minimum sur « Fair »

Dans le cas où la page de connexion crash comme ceci :



Recharger simplement la page.

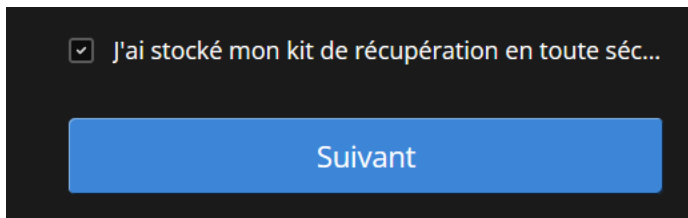


Un kit de sauvegarde sera téléchargé automatiquement une fois la phrase de passe renseignée.

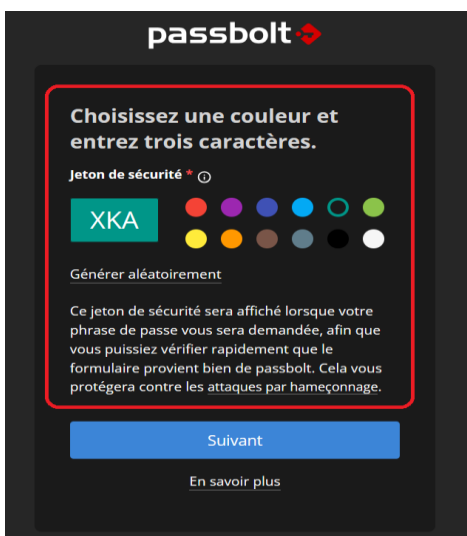


Ce kit permet de récupérer le compte dans le cas d'un oubli de MDP. Il permet aussi de se connecter à Passbolt depuis un autre appareil.

Une fois le kit stocké, il ne vous reste plus qu'à valider.

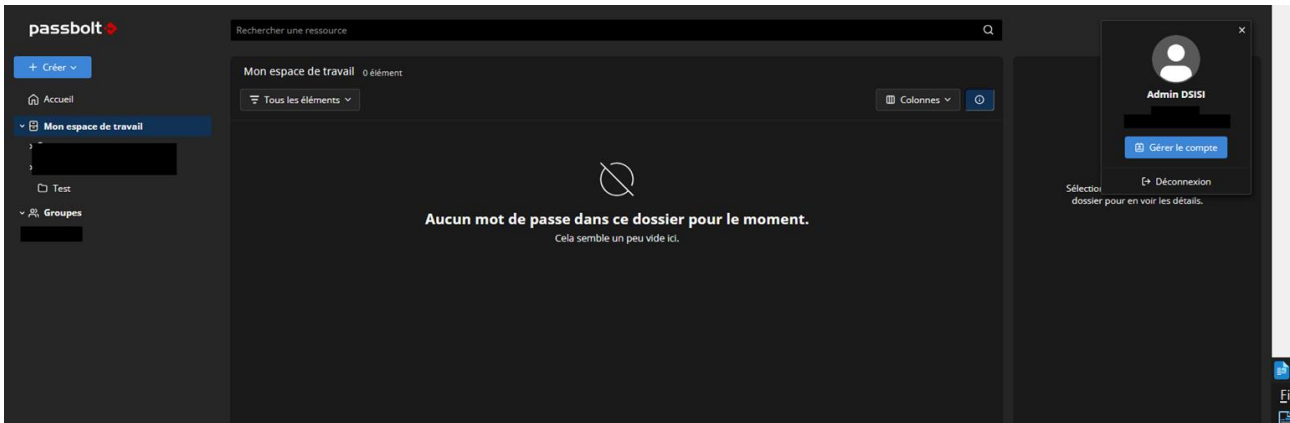


Pour finir, un jeton de sécurité devra être créé.





Passbolt est maintenant prêt à être utilisé.

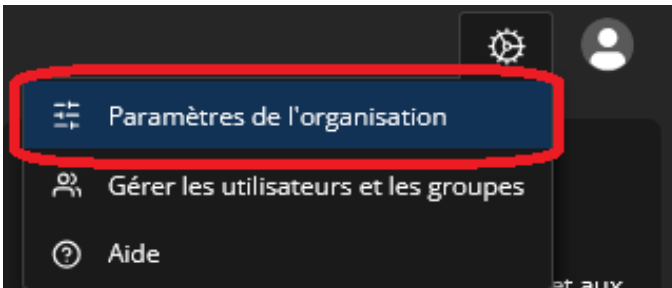




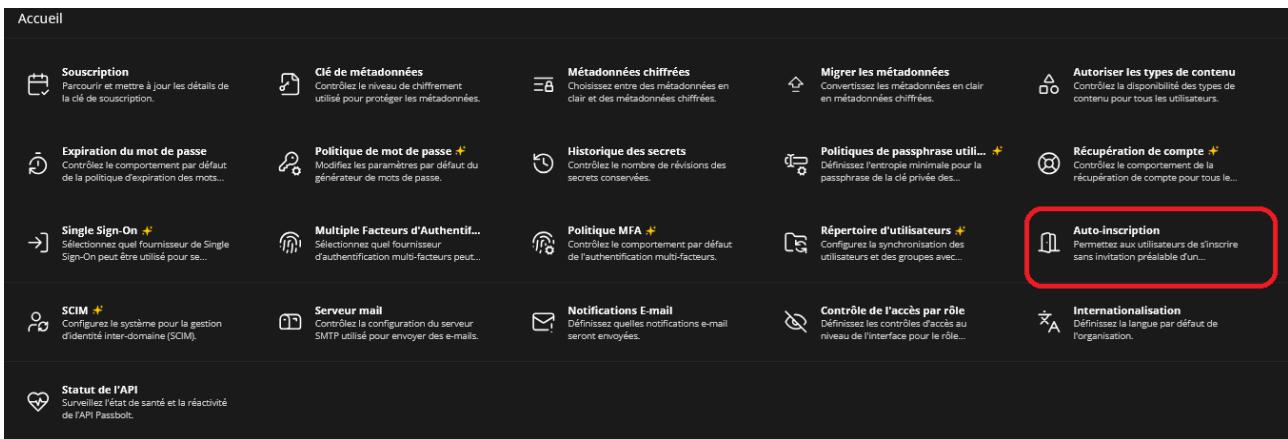
6. Configuration de l'inscription mail

Un dernier point est à régler sur cette configuration de Passbolt. En effet, il est important de paramétrer les domaines autoriser à se connecter à la base.

Étape 1 : Dans la page d'accueil, se rendre en haut à droit sur la roue crantée, puis sélectionner « Paramètres de l'organisation ».

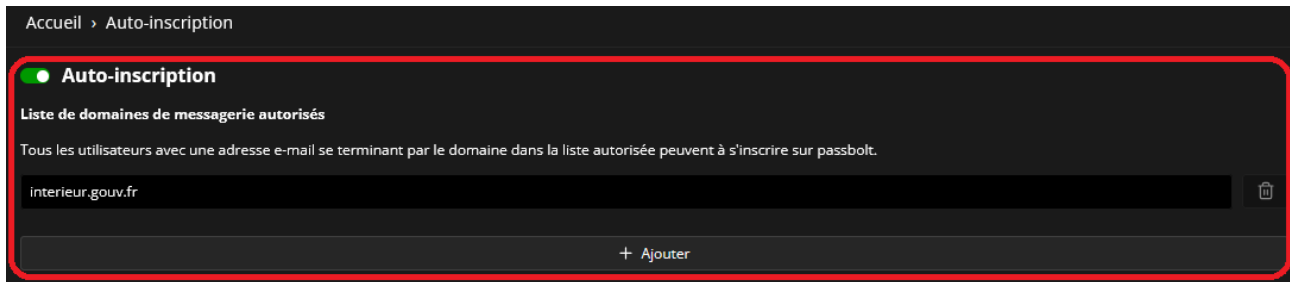


Étape 2 : Aller ensuite dans « Auto-inscription »

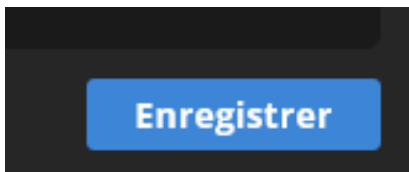




Étape 3 : Une fois dans la page d'autorisation, cocher l'option d'auto-inscription. Puis, renseigner le domaine souhaité.



Enfin, valider avec « Enregistrer ».





7. Difficultés rencontrées

7.1 Problème de nom de domaine

Dans le healthcheck du Passbolt, il nous est dit que le `/healthcheck/status` est inaccessible en raison d'un mauvais nom de domaine renseigné. Il faut donc pour cela ajouter une ligne dans le fichier `hosts`. Il est accessible sur la VM avec la commande suivante :

`sudo nano /etc/hosts` Le fichier est le suivant :

```
GNU nano 8.4 /etc/hosts *
127.0.0.1 localhost
passbolt.sgami SGAMI-N-
```

ajouter en dessous du `localhost` la ligne suivante :

`127.0.0.1 nom.de.domaine.passbolt`

```
GNU nano 8.4 /etc/hosts
127.0.0.1 localhost
127.0.0.1 passbolt.sgami .fr
passbolt.sgami .fr SGAMI-N-
```

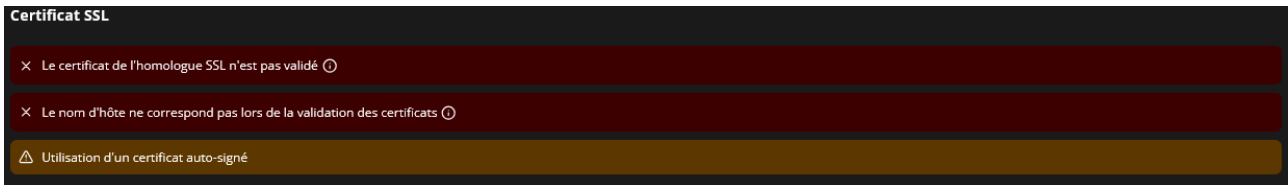
Sauvegarder la modification avec `Ctrl + X` et confirmer avec « Y » ou « O ».

Enfin, redémarrer le service WEB avec `sudo systemctl resart nginx`



7.2 Certificats SSL non reconnus

Voici le problème affiché sur la fenêtre de statuts API sur le Passbolt.



Ce code erreur est dû au fait que le certificat donné au moment de la configuration provient d'une autorité d'organisation + un certificat intermédiaire provenant de cette même autorité.

Pour régler ce problème, il faut donc faire un certificat `fullchain.pem` avec les 2 précédents certificats en son sein.

Puis, convertir le fichier `.pem` en fichier `.crt`

Pour finir, déplacer le certificat `fullchain.crt` dans le dossier `/usr/local/share/ca-certificate`

Une fois ces étapes faites, lancer la commande `sudo update-ca-certificates` puis redémarrer le service WEB.