

# Authentication via Privacyidea



## 1. Mise à jour du système

Avant tout, mets à jour les paquets existants :

```
zafar@auth-srv:~$ sudo apt update && sudo apt upgrade -y
```

les outils nécessaires sont installés :

```
zafar@auth-srv:~$ sudo apt install -y wget gnupg software-properties-common
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
wget est déjà la version la plus récente (1.21.4-1ubuntu4.1).
wget passé en « installé manuellement ».
gnupg est déjà la version la plus récente (2.4.4-2ubuntu17).
gnupg passé en « installé manuellement ».
software-properties-common est déjà la version la plus récente (0.99.49.1).
software-properties-common passé en « installé manuellement ».
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  libllvm17t64
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 2 non mis à jour.
zafar@auth-srv:~$
```

## Objectif

- 1 Un utilisateur tente de se connecter à Guacamole
- 2 Guacamole redirige la connexion vers PrivacyIDEA
- 3 PrivacyIDEA envoie un OTP par e-mail
- 4 L'utilisateur entre son OTP et accède à Guacamole

## 2. Ajouter le dépôt de privacyIDEA

Comme il n'existe pas encore de dépôt officiel pour **Ubuntu 24.04 (Noble)**, on va utiliser le dépôt de **Ubuntu 22.04 (Jammy)** :

Télécharger la clé GPG du dépôt :

Puis on déplace la clé dans le bon dossier avec les privilèges root

```
zafar@auth-srv:~$
wget https://lancelot.netknights.it/NetKnights-Release.asc
--2025-02-03 08:34:41-- https://lancelot.netknights.it/NetKnights-Release.asc
Resolving lancelot.netknights.it (lancelot.netknights.it)... 46.4.108.34
Connecting to lancelot.netknights.it (lancelot.netknights.it)|46.4.108.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3096 (3,0K) [application/octet-stream]
Saving to: 'NetKnights-Release.asc'

NetKnights-Release.asc      100%[=====] 3,02K  --.-KB/s  in 0s
2025-02-03 08:34:41 (908 MB/s) - 'NetKnights-Release.asc' saved [3096/3096]

zafar@auth-srv:~$ sudo mv NetKnights-Release.asc /etc/apt/trusted.gpg.d/
zafar@auth-srv:~$ ls /etc/apt/trusted.gpg.d/
NetKnights-Release.asc  ubuntu-keyring-2012-cdimage.gpg  ubuntu-keyring-2018-archive.gpg
zafar@auth-srv:~$
```

On voit **NetKnights-Release.asc**, c'est bon 👍

Maintenant que la clé est bien ajoutée, on peut passer à l'étape suivante en ajoutant le dépôt et en mettant à jour :

```
zafar@auth-srv:~$ echo "deb http://lancelot.netknights.it/community/jammy/stable jammy main" | sudo tee /etc/apt/sources
.list.d/privacyidea.list
deb http://lancelot.netknights.it/community/jammy/stable jammy main
zafar@auth-srv:~$ sudo apt update
Atteint :1 http://security.ubuntu.com/ubuntu noble-security InRelease
Atteint :2 http://archive.ubuntu.com/ubuntu noble InRelease
```

Installer privacyIDEA avec Apache

```
zafar@auth-srv:~$ sudo apt install -y privacyidea-apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est
```



```

zafar@auth-srv:~$ dpkg -l | grep privacyidea
ii  privacyidea          3.10.2-1jammy          amd64        two-factor authentication
system e.g. for OTP devices
iF  privacyidea-apache2  3.10.2-1jammy          all          2FA system. This is a meta
package to install privacyidea with apache2
zafar@auth-srv:~$

```

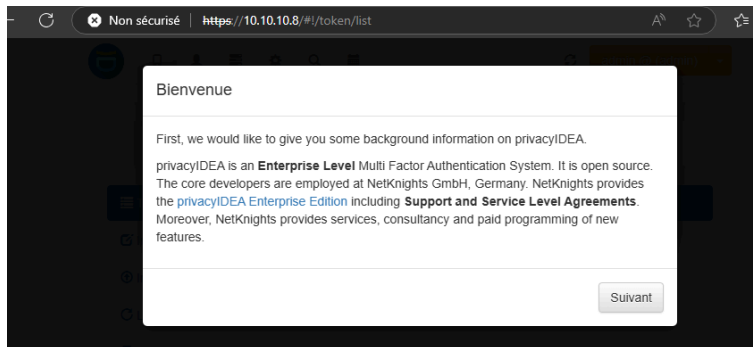
```

zafar@auth-srv:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: zafar
Password:
==== AUTHENTICATION COMPLETE ====
zafar@auth-srv:~$

```

Accéder à

l'interface web 👍



Configurer le serveur SMTP dans privacyIDEA :

Créer un nouveau serveur SMTP smtp-mibc-fr-07.mailinblack.com

Identifiant:   
This is the unique identifying name of the SMTP server definition.

IP or FQDN:

Port:

Timeout:

Destinataire du courriel:   
Il s'agit de l'adresse courriel du expéditeur. Habituellement, il doit s'agir d'une adresse courriel identifiant votre systèr

Nom d'utilisateur:   
Si le serveur SMTP nécessite une authentification vous devez spécifier l'utilisateur.

Mot de passe:

Description:

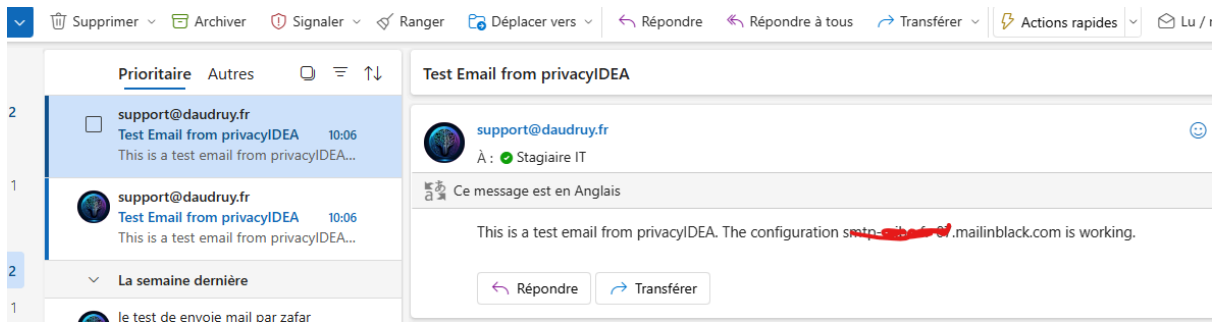
Use StartTLS

Destinataire du test:

Identifiant	IP/FQDN	Destinateur	StartTLS	Description
smtp-mbc-fr-07.mailinblack.com	smtp-mbc-fr-07.mailinblack.com.25	stagiaire-it@daudruy.fr	✓	<a href="#">Supprimer</a>

Configuration Du Système  
 Obtenir La Documentation Du Système  
 Serveurs SMTP  
 Lister Les Définitions Du Serveur SMTP  
 Nouveau Serveur SMTP

Test smtp : 👍



Privacyidea a besoin une base et il peut aller chercher les user sur la bas de guacamole

### Trouver la structure de la table des utilisateurs dans MySQL/MariaDB

Pour que PrivacyIDEA puisse récupérer les utilisateurs, on doit voir comment Guacamole stocke ses comptes.

Sur guacamole on cree un user :

```
MariaDB [guacadb]> CREATE USER 'privacyidea'@'10.10.10.8' IDENTIFIED BY 'zafar';
Query OK, 0 rows affected (0,002 sec)

MariaDB [guacadb]> GRANT ALL PRIVILEGES ON guacadb.* TO 'privacyidea'@'10.10.10.8';
Query OK, 0 rows affected (0,002 sec)

MariaDB [guacadb]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [guacadb]> SHOW GRANTS FOR 'privacyidea'@'10.10.10.8';
+-----+
| Grants for privacyidea@10.10.10.8 |
+-----+
| GRANT USAGE ON *.* TO `privacyidea`@`10.10.10.8` IDENTIFIED BY PASSWORD '*EE159D4B82B52E5C9F27A79925E9E29BB7B840A6' |
| GRANT ALL PRIVILEGES ON `guacadb`.* TO `privacyidea`@`10.10.10.8` |
+-----+
2 rows in set (0,000 sec)

MariaDB [guacadb]> |
```

Sur guacamole Si MySQL n'écoute que sur 127.0.0.1, il faut modifier la config.

```
GNU nano 6.2 /etc/mysql/mariadb.conf.d/50-server.cnf
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0

#
```

Ouvrir le port 3306 dans le pare-feu Autorise PrivacyIDEA (10.10.10.8) à accéder à MySQL :

```
zafar@apache-guaca:~# sudo ufw allow from 10.10.10.8 to any port 3306 proto tcp
Rule added
zafar@apache-guaca:~# sudo ufw status
Status: active

To                Action              From
--                -
3389              ALLOW              Anywhere
4822              ALLOW              Anywhere
8080              ALLOW              Anywhere
22               ALLOW              Anywhere
80/tcp           ALLOW              Anywhere
443/tcp          ALLOW              Anywhere
80               ALLOW              Anywhere
443              ALLOW              Anywhere
3306/tcp         ALLOW              10.10.10.8
```

On test la connexion a la base depuis Privacyidea :

```
zafar@auth-srv:~$ mysql -u privacyidea -p -h 10.10.10.4 -D guacadb
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 31
Server version: 5.5.5-10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> exit
Bye
```

# Configuration du **résolveur SQL** dans PrivacyIDEA pour récupérer les utilisateurs depuis **guacamole\_user**.

The screenshot shows the 'Modifier l'interpréteur SQL privacyidea' configuration page. The form includes the following fields:

- Nom de l'interpréteur: `privacyidea`
- Pilote: `mysql+pymysql`
- Serveur: `10.10.10.4` (Port: `3306`)
- Base de données: `guacadb`
- User: `privacyidea`
- Mot de passe: `.....`

Below the form, there is a checkbox for 'Modifier l'utilisateur de la base' and a note: 'The user data in this database can be modified from within privacyIDEA.' Below that, there are buttons for application types: Wordpress, OTRS, Tine 2.0, Owncloud, Typo3, and Drupal. The 'Tableau' field is set to `guacamole_user` (Limite: `500`). The 'Mapping' field contains the JSON string: `{ "userid": "user_id", "username": "full_name", "email": "email_address" }`.


The screenshot shows the 'Utilisateurs' section of the PrivacyIDEA interface. A table lists the configured resolvers:

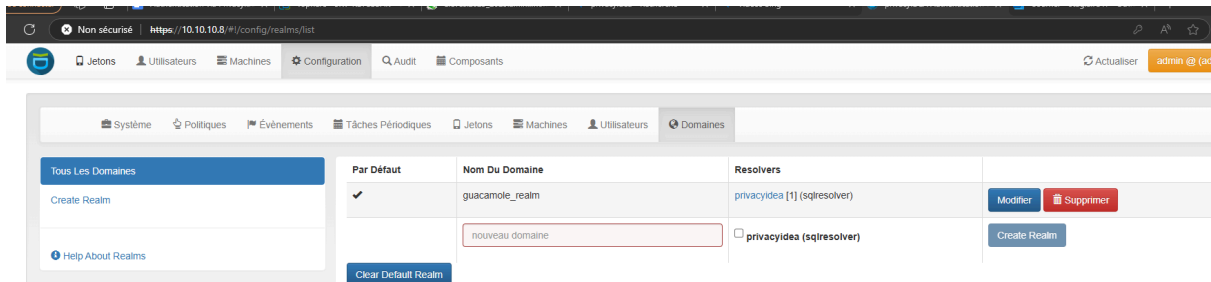
Nom De L'interpréteur	Type	Actions
privacyidea	sqlresolver	<a href="#">Modifier</a> <a href="#">Supprimer</a>

A notification at the top right of the interface states 'Found 2 users.' The left sidebar shows navigation options for various resolver types, with 'Nouveau Sqiresolver' highlighted.

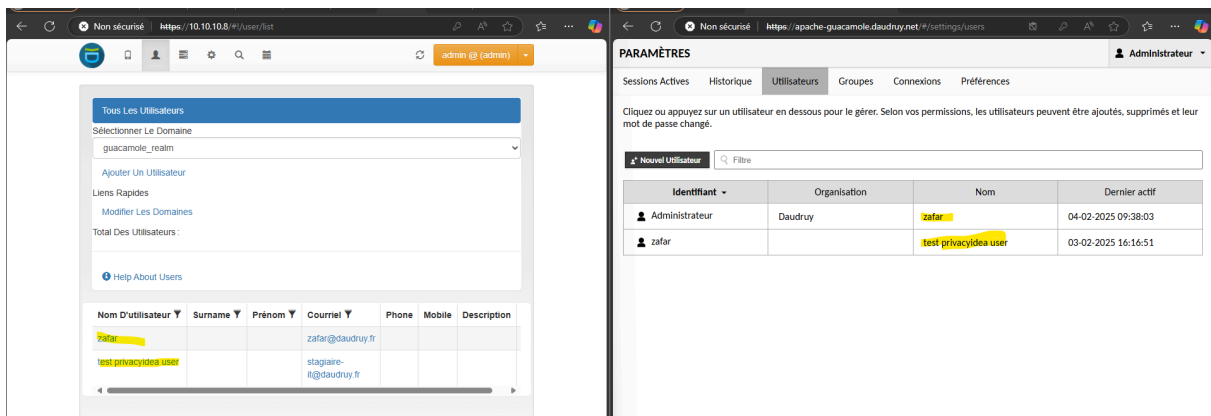
## Créer un domaine (Realm) dans PrivacyIDEA

Un **realm** est un groupe d'utilisateurs géré par PrivacyIDEA. On doit lier notre résolveur SQL à un domaine.

 **Objectif** : Quand un utilisateur essaie de se connecter, PrivacyIDEA va chercher les comptes dans `guacamole_mysql`.



Vérifier que PrivacyIDEA trouve bien les utilisateurs du Realm



Modifier Guacamole pour pointer vers le bon Realm

Super ! 🎉 Maintenant que **PrivacyIDEA récupère bien les utilisateurs de Guacamole via le domaine `guacamole_realm`**, voici les dernières étapes pour finaliser l'authentification OTP.



## Activer l'authentification OTP pour les utilisateurs

On crée un politique de authentification

The screenshot shows the 'Modifier la politique OTP\_Email\_Auth\_guacamole' page. The page has a navigation bar with 'Système', 'Politiques', 'Événements', 'Tâches Périodiques', 'Jetons', 'Machines', 'Utilisateurs', and 'Domaines'. The main content area is titled 'Modifier la politique OTP\_Email\_Auth\_guacamole' and includes buttons for 'Désactiver' and 'Supprimer'. The form fields are: 'Nom de la politique' (OTP\_Email\_Auth\_guacamole), 'Scope' (authentication), 'Priorité' (1), and 'Description' (Politique pour l'envoi d'OTP par e-mail à Guacamole). There is a '+ Créer une politique' button at the bottom right.

Puis on intègre notre domaine et le user qui vas chercher le user dans guacamole

The screenshot shows the 'Condition' tab of the policy configuration. It includes a '+ Créer une politique' button at the top right. The 'Condition' section has the following fields: 'User-Realm' (guacamole\_realm), 'User-Resolver' (privacyidea), 'User' (userA, userB), 'Username case-insensitive.' (checkbox), 'privacyIDEA Nodes' (None Selected), 'Client' (10.0.0.0/8, 110.0.0.124), and 'Valid time' (Mon-Fri: 9-18, Sat: 10-15). There is a checkbox 'Check all possible resolvers of a user to match the resolver in this policy.' which is checked. Below this is a table for 'Conditions supplémentaires' with columns: Actif, Section, Clé, Comparateur, and Valeur.

Dans la section **Action**, on cherche ces paramètres et configurer-les :

The screenshot shows the 'Action' tab of the policy configuration. It includes the following parameters and their configurations:

- emailautosend**: S'il est défini, un nouveau mot de passe à usage unique de courriel sera envoyé après une authentification réussie avec un mot de passe précédemment envoyé par courriel.
- emailsubject**: L'objet du courriel pour un jeton de courriel. Utilisez {otp} et {serial} comme paramètres. Configuration: Votre code OTP pour
- emailtext**: Le texte qui sera envoyé par courriel pour un jeton de courriel. Utilisez {otp} et {serial} comme paramètres. Vous pouvez également spécifier un nom de fichier comme modèle de courriel commençant par « file: ». Configuration: Bonjour, Votre code
- enroll via multichallenge**: In case of a successful authentication the following token is enrolled. The maximum number of tokens for a user is

Clé : `emailautosend`

📌 Cela permet d'envoyer un OTP automatiquement à chaque tentative de connexion.

Clé : `emailsubject`

Valeur : Votre code OTP pour la connexion à Guacamole

Clé : `emailtext`

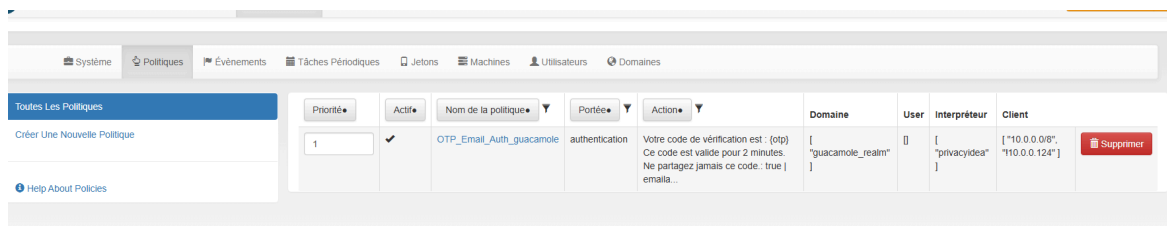
Valeur : Bonjour,

Votre code de vérification est : `{otp}`

Ce code est valide pour 2 minutes.

Ne partagez jamais ce code.

📌 `{otp}` est un paramètre dynamique qui sera remplacé par le code OTP.



Priorité	Actif	Nom de la politique	Portée	Action	Domaine	User	Interpréteur	Client	
1	✓	OTP_Email_Auth_guacamole	authentication	Votre code de vérification est : {otp} Ce code est valide pour 2 minutes. Ne partagez jamais ce code.: true   emalla...	[ "guacamole_realm" ]	[]	[ "privacyidea" ]	[ "*10.0.0.0/8", "*10.0.0.124" ]	<a href="#">Supprimer</a>

## Vérifier que l'OTP est bien actif pour chaque utilisateur



Informations sur l'utilisateur test privacyidea user dans le domaine guacamole\_realm

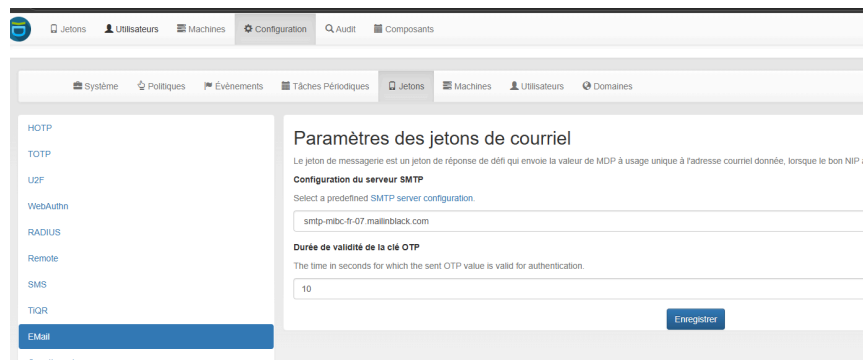
nom d'utilisateur: test privacyidea user, courriel: stagiaire.n@caudray.fr

Custom attributes for user test privacyidea user

Assigner un nouveau jeton

Numéro de série	Type	Actif	Window	Description	Falloccounter	Maxtail	Otpien	Container

## Le smtp



Paramètres des jetons de courriel

Configuration du serveur SMTP

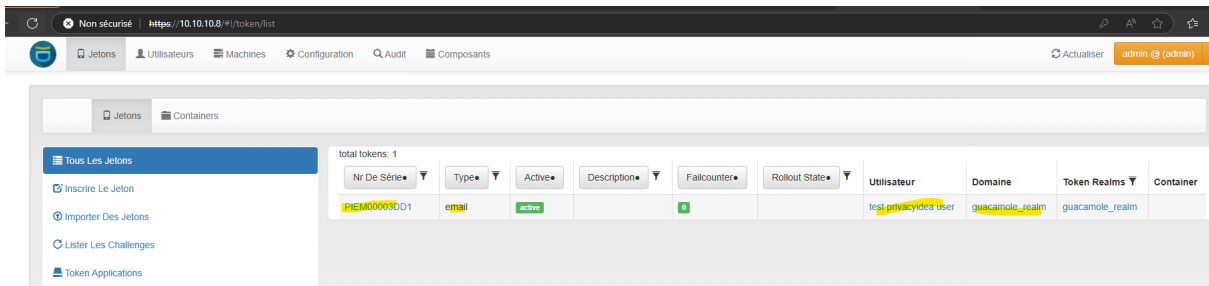
smtp-mbc-fr-07.mallinblack.com

Durée de validité de la clé OTP

10

Enregistrer

l'utilisateur a bien un "Jeton OTP Email" actif



PrivacyIDEA est bien configuré (SMTP, SQL Resolver, Politique OTP), mais il faut maintenant l'intégrer avec Guacamole pour que l'authentification OTP fonctionne.

## Télécharger et installer l'extension OpenID sur guacamole

```
zafar@apache-guaca:~# wget https://dlcdn.apache.org/guacamole/1.5.5/binary/guacamole-auth-sso-1.5.5.tar.gz
--2025-02-04 09:19:40-- https://dlcdn.apache.org/guacamole/1.5.5/binary/guacamole-auth-sso-1.5.5.tar.gz
Resolving dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38286364 (37M) [application/x-gzip]
Saving to: 'guacamole-auth-sso-1.5.5.tar.gz'

guacamole-auth-sso-1.5.5. 100%[=====] 36,51M 87,5MB/s in 0,4s

2025-02-04 09:19:41 (87,5 MB/s) - 'guacamole-auth-sso-1.5.5.tar.gz' saved [38286364/38286364]

zafar@apache-guaca:~# ls
apacheguac.conf apacheguac.csr dead.letter guac_notify.sh
apacheguac.crt apacheguac.key guacamole-auth-sso-1.5.5.tar.gz
zafar@apache-guaca:~# tar -xvzf guacamole-auth-sso-1.5.5.tar.gz
```

```
zafar@apache-guaca:~# sudo cp guacamole-auth-sso-1.5.5/openid/guacamole-auth-sso-openid-1.5.5.jar /etc/guacamole/extensions/
zafar@apache-guaca:~# ls
apacheguac.conf apacheguac.csr dead.letter guacamole-auth-sso-1.5.5.tar.gz
apacheguac.crt apacheguac.key guacamole-auth-sso-1.5.5 guac_notify.sh
zafar@apache-guaca:~# ls /etc/guacamole/extensions/
guacamole-auth-jdbc-mysql-1.5.5.jar guacamole-history-recording-storage-1.5.5.jar
guacamole-auth-sso-openid-1.5.5.jar
zafar@apache-guaca:~#
```

```
zafar@apache-guaca:~# sudo chown zafar:zafar /etc/guacamole/extensions/guacamole-auth-sso-openid-1.5.5.jar
zafar@apache-guaca:~# sudo chmod 644 /etc/guacamole/extensions/guacamole-auth-sso-openid-1.5.5.jar
zafar@apache-guaca:~# sudo systemctl restart guacd
zafar@apache-guaca:~# sudo systemctl restart tomcat9
```

```
#####
# déclaration de de la connexion a Mariadb
# ce fichier est utile aussi pour d'autre parametres

# MySQL -----
#mysql-hostname: 127.0.0.1
#mysql-port: 3306
#mysql-database: guacadb
#mysql-username: userdb
#mysql-password: zafar
#-----

history-recording-enabled: true
history-recording-storage-dir: /var/lib/guacamole/recordings

auth-provider: net.sourceforge.guacamole.net.auth.openid.OpenIDAuthenticationProvider
openid-issuer: http://10.10.10.8
openid-authentication-uri: http://10.10.10.8/validate/check
openid-client-id: admin
openid-client-secret: admin
openid-redirect-uri: https://10.10.10.4/guacamole/
openid-scope: openid email profile
openid-username-claim-type: sub
openid-realm: guacamole_realm
openid-authorization-endpoint: http://10.10.10.8/validate/check
openid-userinfo-endpoint: http://10.10.10.8/validate/check
openid-authorization-endpoint: https://10.10.10.8/validate/check
openid-userinfo-endpoint: http://10.10.10.8/validate/check?user={USERNAME}
openid-login-form: true
```

## Compte Rendu – Configuration de l'authentification OpenID avec PrivacyIDEA

Date : 04/02/2025

Dans le cadre de mon stage, j'ai entrepris la mise en place d'une authentification OpenID avec PrivacyIDEA pour Guacamole. Après configuration, la redirection depuis Guacamole vers PrivacyIDEA fonctionne correctement. Cependant, un problème persiste : PrivacyIDEA ne reçoit pas correctement l'utilisateur et retourne l'erreur **ERR905**, empêchant l'authentification finale.

L'une des exigences était **l'utilisation obligatoire du serveur SMTP et des adresses e-mail de l'entreprise** pour l'envoi des OTP. Cette contrainte a complexifié la configuration et nécessité plus de temps pour la recherche et l'adaptation du système.

Étant dans ma dernière semaine de stage, je ne peux pas poursuivre cette tâche, car d'autres priorités restent à traiter, notamment :

- **Mettre Guacamole sur Internet**
- **Configurer le NAT et le Proxy**

Comme cette implémentation d'OpenID ne faisait pas partie du cahier des charges initial, je vais proposer une alternative plus simple et mieux adaptée :

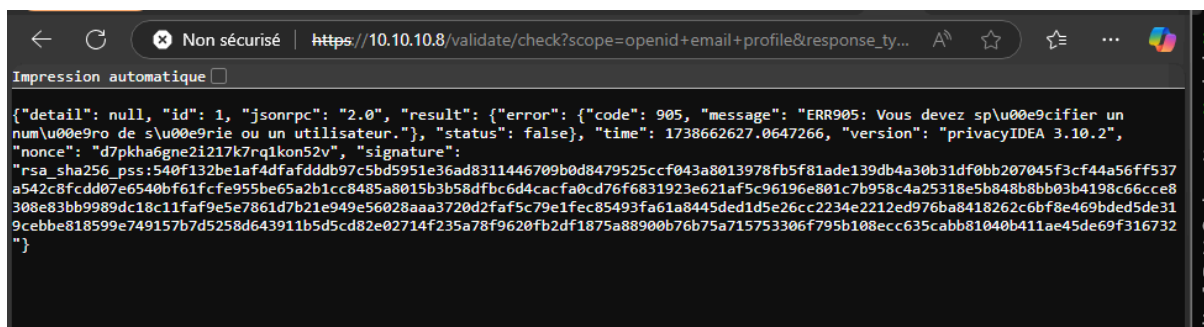
**l'authentification TOTP** recommandée par Guacamole.

## Bilan des apprentissages

Malgré les difficultés rencontrées, cette configuration m'a permis d'acquérir des connaissances approfondies sur les différentes méthodes d'authentification et leur intégration, notamment :

- **Les protocoles d'authentification OpenID, TOTP et LDAP**
- **L'intégration de PrivacyIDEA avec Guacamole**
- **Les contraintes liées à l'authentification en entreprise (SMTP, sécurité, gestion des identités)**

Cette expérience m'a permis de mieux comprendre les défis de l'authentification avancée et la gestion des accès en entreprise.



```
Non sécurisé | https://10.10.10.8/validate/check?scope=openid+email+profile&response_ty...
Impression automatique
{"detail": null, "id": 1, "jsonrpc": "2.0", "result": {"error": {"code": 905, "message": "ERR905: Vous devez sp\u00e9cifier un num\u00e9ro de s\u00e9rie ou un utilisateur."}, "status": false}, "time": 1738662627.0647266, "version": "privacyIDEA 3.10.2", "nonce": "d7pkha6gne2i217k7rq1kon52v", "signature": "rsa_sha256_pss:540f132be1af4dfafdddb97c5bd5951e36ad8311446709b0d8479525ccf043a8013978fb5f81ade139db4a30b31df0bb207045f3cf44a56ff537a542c8fcd07e6540bf61fcfe955be65a2b1cc8485a8015b3b58dfbc6d4cacfa0cd76f6831923e621af5c96196e801c7b958c4a25318e5b848b8bb03b4198c66cce8308e83bb9989dc18c11faf9e5e7861d7b21e949e56028aaa3720d2faf5c79e1fec85493fa61a8445ded1d5e26cc2234e2212ed9776ba8418262c6bf8e469bde5de319ceb818599e749157b7d5258d643911b5d5cd82e02714f235a78f9620fb2df1875a88900b76b75a715753306f795b108ecc635cabb81040b411ae45de69f316732"}
}
```

Sources :

[3. First Steps — privacyIDEA 3.10dev1 documentation](#)

[privacyidea/doc/installation/ubuntu.rst at master · privacyidea/privacyidea · GitHub](#)