

Configuration d'une authentification SAML pour Guacamole

Lien : <https://guacamole.apache.org/doc/gug/saml-auth.html>

Installation de l'extension SAML pour guacamole

- Téléchargez guacamole-auth-sso-1.6.0.tar.gz, décompressez l'archive et déplacez guacamole-auth-sso-saml-1.6.0.jar dans le dossier extensions :

```
wget https://d1cdn.apache.org/guacamole/1.6.0/binary/guacamole-auth-sso-1.6.0.tar.gz
tar -xzf guacamole-auth-sso-1.6.0.tar.gz
sudo mv guacamole-auth-sso-1.6.0/saml/guacamole-auth-sso-saml-1.6.0.jar /etc/guacamole/extensions/
```

Publier l'application dans Azure

- Accéder au portail Azure → Microsoft Entra ID → Applications d'entreprise.
- Nouvelle application → Créer votre propre application.
- Choisir **Configurer le proxy d'application pour un accès à distance sécurisé à une application locale**

Essentiel Avancé

Mode Maintenance ⓘ

URL interne ⓘ *

URL externe ⓘ

https:// ▾

-educvaladonlimogesfr.msapproxy.net/ ▾



Segments d'application ⓘ

Ajouter des segments d'application

Pré-authentification ⓘ

Groupe de connecteurs ⓘ

Configurer l'authentification SAML

- Accéder à l'application créée
- Dans l'application créée → Authentification unique → SAML.
- Renseigner :
 - Identificateur (Entity ID) : fourni par le service.
 - URL de réponse (ACS) : fourni par le service.
 - URL de connexion (facultatif) : page de login du service.

Télécharger le fichier de métadonnées XML d'Entra ID (il contient le certificat et les endpoints).

Configurer le service web avec les infos Entra ID

- Modifiez guacamole.properties avec les valeurs Azure :
 - saml-idp-metadata-url: <App Federation Metadata Url>
 - saml-entity-id: <https://guacamole.votre-domaine.com/>
 - saml-callback-url: <https://guacamole.votre-domaine.com/api/ext/saml/callback>
 - saml-debug: true
- Fournir au service :
 - Entity ID d'Entra ID (souvent <https://sts.windows.net/{tenant-id}/>).
 - SSO URL : <https://login.microsoftonline.com/{tenant-id}/saml2>.
 - Certificat public (X.509) pour vérifier les signatures.

Importer le metadata XML d'Entra ID si le service le supporte.

□ 5. Attribuer des utilisateurs

Dans Entra ID → Utilisateurs et groupes → attribuer les comptes qui peuvent se connecter.

□ 6. Tester la connexion

Utiliser le bouton Tester l'authentification unique dans Azure. Vérifier les logs SAML (ACS du service) pour les assertions.

□ Points clés

Format des claims : Par défaut, Entra ID envoie NameID (UPN). Vous pouvez personnaliser les attributs dans Attributs et revendications.
Certificat : Surveillez la rotation automatique (Azure change le certificat tous les 3 ans). Sécurité : Activez la signature des assertions et la validation des audiences.

- Modification du fichier **guacamole.properties** pour configurer SAML.

```
sudo nano /etc/guacamole/guacamole.properties
```

- Ajoutez dans ce fichier les lignes suivantes :

```
# MySQL
mysql-hostname: 127.0.0.1
mysql-port: 3306
mysql-database: guacamole_db
mysql-username: guacamole_user
mysql-password: P@$w0rd2025Secure
```

- Déclarez le serveur Guacamole (ici, on déclare une connexion locale sur le port par défaut, à savoir 4822).

```
sudo nano /etc/guacamole/guacd.conf
```

- Voici le code à intégrer :

```
[server]
bind_host = 0.0.0.0
bind_port = 4822
```

- Redémarrez les trois services liés à Apache Guacamole :

```
sudo systemctl restart tomcat9 guacd mariadb
```

From:
/ - **Les cours du BTS SIO**

Permanent link:
</doku.php/reseau/cloud/accesdistance/guacamoleauthsaml?rev=1768225353>

Last update: **2026/01/12 14:42**

