

Multifactor Authentication (MFA)

Seul un paramètre est nécessaire afin de le mettre en place

\$home/etc/cas/config/cas.properties

```
# MFA, mfa-gauth est un exemple possible, les valeurs possibles sont 'mfa-duo', 'mfa-authy' etc...
cas.authn.mfa.globalProviderId=mfa-gauth
```

Pour tester (sinon ne fonctionnera pas): <http://mydomain.com/cas/login?service=https://google.fr>

Activer l'authentification par service

Il est nécessaire de créer un nouveau fichier utilisant l'overlay.

Ajouter le fichier

\$home/cas/src/main/resources/services/gauth.json

```
{
  "@class" : "org.apereo.cas.services.RegexRegisteredService",
  "serviceId" : "^(https|imaps)://.*",
  "name" : "pam",
  "id" : 9999,
  "description" : "Get the uid attribute from LDAP",
  "evaluationOrder" : 9999,
  "multifactorPolicy" : {
    "@class" : "org.apereo.cas.services.DefaultRegisteredServiceMultifactorPolicy",
    "multifactorAuthenticationProviders" : [ "java.util.LinkedHashSet", [ "mfa-gauth" ] ]
  }
}
```

Sachez qu'un seul fichier par service sera activé (il est possible de voir sur la page de login par default le nom apparaître), ce qui signifie que ce fichier doit aussi contenir toute autre configuration concernant ce service.

L'argument **"multifactorAuthenticationProviders"** : [**"java.util.LinkedHashSet"**, [**"mfa-gauth"**]] définira à présent l'authentification donc le cas. properties doit être mis à jour et la propriété `cas.authn.mfa.globalProviderId=mfa-gauth` peut être supprimée.