

# Intégration de PRONOTE.net dans un ENT

Cette intégration permet aux parents, professeurs, élèves ... d'accéder aux données publiées par PRONOTE.net à travers un Environnement Numérique de Travail en ne s'authentifiant qu'une seule fois.

## 1 . Paramétrage de PRONOTE.net pour un ENT utilisant CAS

Le paramétrage s'effectue dans **Intégration dans un ENT > Authentification avec CAS**.

La clé de chiffrement doit être la même que celle saisie dans l'onglet **Sécurité** de PRONOTECas (Voir page 1).

**Intégration dans un ENT**

Authentification avec CAS | Authentification sans CAS |

**Clé de chiffrement**  
Vous devez saisir le mot de passe utilisé pour le chiffrement de la communication entre PRONOTECas et PRONOTE.net.

Clé de chiffrement : [.....] [Remplacer]

**Liste des adresses IP autorisées**  
Vous devez indiquer les adresses IP des postes où sont installés PRONOTE cas, autorisés à interroger PRONOTE.net.

192.168.200.120
192.168.200.36

Conserver dans des fichiers journaux l'historique de toutes les connexions  
 Concernant la fédération d'identités, n'enregistrer que les échecs

Saisissez la (ou les) adresse(s) IP du ou des postes où est installé PRONOTECas (seules machines autorisées à interroger PRONOTE.net).

Cochez cette option pour conserver un historique de toutes les connexions de toutes les connexions à PRONOTE.net effectuées à travers CAS.

## 2 . Configuration de PRONOTECas

### Pré-requis

Vous devez disposer d'un serveur Tomcat version 5.5 et de JRE à partir de la version 1.5.

### 2.1. Installation de PRONOTECas

- 1 Sur la page **Téléchargement > PRONOTE** du site Internet [www.index-education.com](http://www.index-education.com), cliquez sur **PRONOTECas**.
- 2 Si votre ENT s'interface avec les PRONOTE.net de plusieurs établissements, spécifiez le nom de l'établissement à utiliser pour générer le nom de l'application qui sera créé par le serveur Tomcat.
- 3 Choisissez le répertoire de destination du fichier \*.war, il s'agit du répertoire /webapps de la machine où est installée le serveur Tomcat.

### 2.2. Première connexion à PRONOTECas

- 1 Depuis un navigateur web, saisissez l'URL de l'application créée par le serveur Tomcat.  
**URL\_DeLaMachineAbitrantLeServeurTomcat/NomDonnéAuFichierWar.**
- 2 Vous accédez à la page de connexion de PRONOTECas.
- 3 Saisissez le mot de passe par défaut : **adminpronote**.
- 4 PRONOTECas s'ouvre.

Mot de passe : [.....]

### Modifier le mot de passe administrateur

Dès la première connexion, nous vous conseillons de saisir un nouveau mot de passe.

**Saisie du mot de passe de l'administrateur PRONOTE cas**

Ancien mot de passe : [.....]

Nouveau mot de passe : [.....]

Nouveau mot de passe : [.....]

---

**Saisie de la clé de chiffrement pour les communications avec PRONOTE.net**

Clé de chiffrement\* : [.....]

\* champ obligatoire

La clé de chiffrement saisie ici doit être strictement la même que celle saisie dans l'onglet **Connexion à travers CAS** de PRONOTE.net. Elle permet de crypter la communication entre les deux applications.

Le bouton **Valider** ne devient actif que lorsque vous avez rempli tous les champs obligatoires de configuration dans les onglets **Paramètres généraux** et **Sécurité**. Pour mieux les distinguer, ils sont marqués d'un astérisque (\*).

Lorsque vous validez la modification, Tomcat recharge le contexte de PRONOTECas.

**Mise en garde :** Selon la configuration de votre serveur Tomcat, il se peut qu'il n'autorise pas le rechargement automatique. Dans ce cas, vous devez le redémarrer manuellement.

## Configurer les paramètres généraux

L'onglet **Paramètres généraux** permet de configurer PRONOTE.net et le serveur CAS auprès desquels PRONOTEcas se connecte.

Saisissez l'**Adresse** (publique ou privée) utilisée pour la fédération d'identité (le troisième champs permet, le cas échéant, de spécifier le chemin d'une redirection). Par défaut PRONOTEcas est utilisé comme proxy et relaie aussi les communications entre les espaces et le .net.

En désactivant le mode proxy vous permettez une communication directe à PRONOTE.net. De ce fait, vous devez renseigner son adresse publique.

Renseignez toutes les informations nécessaires à la communication entre PRONOTEcas et le serveur cas. Le protocole HTTPS obligatoire.

Paramètres généraux	Correspondances LDAP	Sécurité	Alerte
<b>Connexion à PRONOTE.net</b>			
Adresse utilisée pour la fédération d'identité* : http:// 192.168.200.120 : 83 /			
<input type="checkbox"/> Désactiver le mode proxy (Par défaut, HYPERPLANNINGcas est utilisé comme proxy)			
Adresse publique de PRONOTE.net : http:// : /			
<b>Connexion au serveur CAS</b>			
Nom d'hôte ou adresse IP du serveur PRONOTEcas* : PRONOTEcas.index-education.france			
URL de la page login du serveur CAS* : https://srv-cas/cas/login			
URL du serveur CAS* : https://srv-cas/cas/			

\* champ obligatoire

## Configurer les correspondances LDAP

L'onglet **Correspondances LDAP** permet de configurer les catégories d'utilisateurs diffusées par le serveur CAS et de les faire correspondre avec les Espaces de PRONOTE.net. Par défaut, PRONOTEcas s'appuie sur les profils nationaux de l'annuaire LDAP du Cahier des charges du Ministère<sup>1</sup>. Cependant, chaque projet ENT est libre de définir des valeurs différentes pour l'attribut "ENTPersonProfils".

Si votre ENT a défini des valeurs particulières pour l'attribut "ENTPersonProfils", vous devez l'indiquer via cet écran de paramétrage.

Il est possible de saisir plusieurs valeurs par champ. Dans ce cas, utilisez le ; comme séparateur.

Paramètres généraux	Correspondances LDAP	Sécurité	Alerte
<b>Correspondance entre les utilisateurs des Espaces PRONOTE et l'annuaire LDAP</b>			
<b>Espaces PRONOTE : Valeurs LDAP</b>			
Professeurs : National_3			
Elèves : National_1			
Parents : National_2			
Entreprises (Maîtres de stage) :			
Académie (Inspecteurs pédagogiques) : National_7			
Vie scolaire (Personnels) :			

\* champ obligatoire

## Configurer les alertes

L'onglet **Alerte** permet de mentionner l'adresse e-mail à laquelle PRONOTEcas doit spécifier les incompatibilités de versions entre PRONOTEcas et PRONOTE.net.

Indiquez que vous souhaitez être prévenu en cas d'incompatibilité de versions.

Renseignez :  
- l'adresse du serveur SMTP  
- le nom que vous souhaitez voir apparaître en tant qu'émetteur,  
- l'e-mail auquel envoyer l'alerte.

Paramètres généraux	Correspondances LDAP	Sécurité	Alerte
<input type="checkbox"/> Me prévenir par e-mail en cas d'erreur liées à des incompatibilités de versions			
<b>Paramètres SMTP nécessaires</b>			
Adresse du serveur SMTP : *			
Nom de l'émetteur : *			
E-mail du destinataire : *			

\* champ obligatoire

Les profils à portée nationale sont définis à la page 55 au chapitre 6 du Cahier des charges de l'Annuaire ENT.

## 2.3. Connexions suivantes

Une fois la configuration effectuée, connectez-vous sur : [URL\\_DeLaMachineAbitantLeServeurTomcat/NomDonnéAuFichierWar/admin.htm](http://URL_DeLaMachineAbitantLeServeurTomcat/NomDonnéAuFichierWar/admin.htm).

En tant qu'administrateur de PRONOTEcas, vous devez vous authentifier auprès de CAS pour accéder à PRONOTEcas.

1. Définition et conception de l'annuaire ENT – Cahier des charges de l'annuaire ENT (document principal) – Version 1.52 du 30 avril 2007.

## 2.4. URL utilisateurs des différents Espaces

L'accès aux différents Espaces se fait par `URL_DeLaMachineAbitantLeServeurTomcat/NomDonnéAuFichierWar/NomEspace.html`

Espace PRONOTE	NomEspace
Elèves	<code>eleve.html</code>
Professeurs	<code>professeur.html</code>
Parents	<code>parent.html</code>
Entreprises	<code>entreprise.html</code>
Académie	<code>academie.html</code>
Vie scolaire	<code>viescolaire.html</code>

Les autorisations de publication des espaces définies au niveau de PRONOTE.net restent valables pour un accès via PRONOTEcas.

# Authentification avec CAS

## 1 . Configuration du serveur Tomcat

En fonction de l'environnement d'exécution du serveur Tomcat, des problèmes d'encodage peuvent survenir dans les pages générées par PRONOTEcas. Pour y remédier, il faut configurer l'encodage au niveau du serveur Tomcat d'exécution de PRONOTEcas.

### Modification de CATALINA\_OPTS

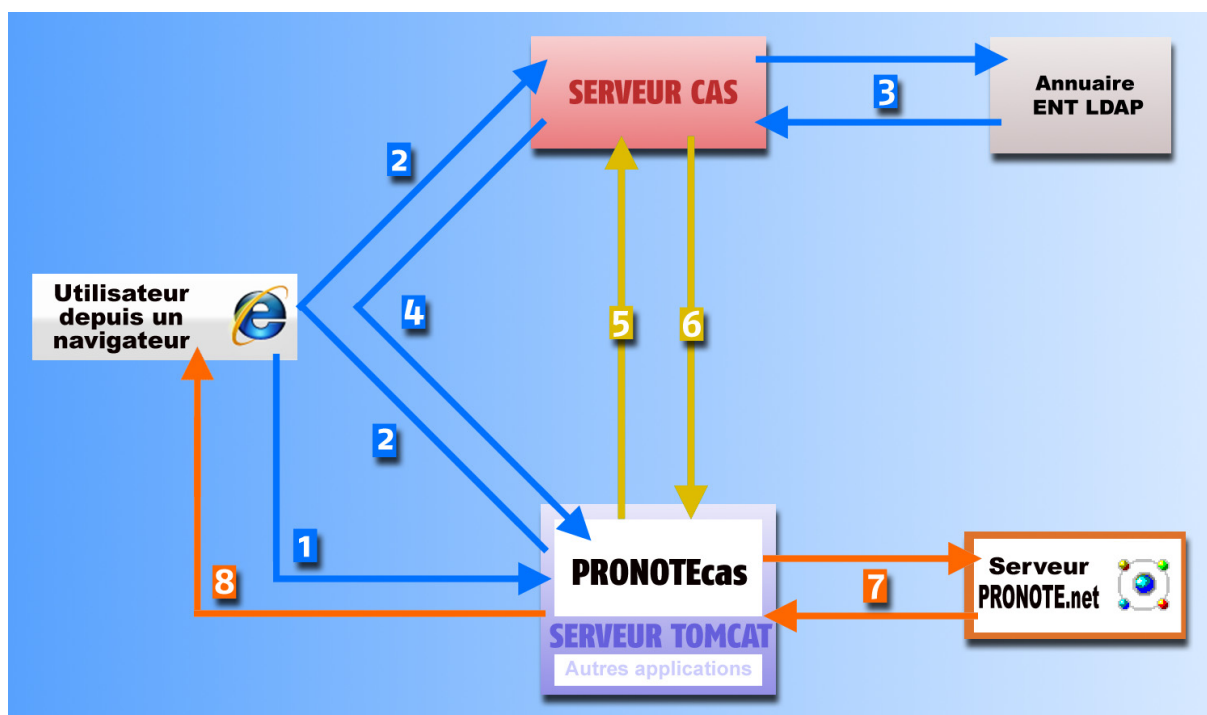
Spécification de l'encodage par modification de la variable d'environnement CATALINA\_OPTS dans le script "catalina.sh" ou "catalina.bat" du serveur Tomcat.

```
CATALINA_OPTS = "-Dfile.encoding=UTF-8"
```

## 2 . Synchronisation des identités entre l'annuaire ENT LDAP et la base de données PRONOTE

Dans le cadre de la CAS-ification de l'application web PRONOTE.net se pose la problématique de synchronisation des informations d'identité entre les deux référentiels de données : l'annuaire ENT LDAP et la base de données PRONOTE.

- 1 L'utilisateur demande l'accès à l'application PRONOTE.net.
- 2 PRONOTEcas redirige la demande du navigateur vers le serveur CAS.
- 3 Le serveur CAS vérifie l'identité de l'utilisateur dans l'annuaire LDAP,
- 4 puis redirige l'utilisateur, avec un ticket CAS, vers PRONOTEcas.
- 5 Avec ce ticket, PRONOTEcas authentifie l'utilisateur auprès du serveur CAS
- 6 qui lui communique un ensemble d'attributs utilisateur extraits de l'annuaire LDAP.
- 7 Ces informations permettent à PRONOTE.net d'identifier l'utilisateur dans son propre système de base de données
- 8 et de renvoyer sa réponse à l'utilisateur.



## Attributs utilisateur de l'annuaire LDAP communiqués par le serveur CAS

Voici la liste des attributs obligatoires ou optionnels utilisés par PRONOTEcas

(en référence au document " Définition et Conception de l'annuaire ENT " - version 1.52 - MENESR 30 avril 2007) :

	Classe LDAP	Attribut LDAP *	Description	Libellé de la balise SAML de validation du ticket CAS *
Commun à tous les utilisateurs	Person	<b>sn</b> (*)	Nom d'usage	<b>nom</b> (*)
	inetOrgPerson	<b>givenName</b> (*)	Prénom usuel	<b>prenom</b> (*)
		<b>uid</b>	Identifiant unique interne à l'ENT	user
	ENTPerson	<b>ENTPersonLogin</b>	Identifiant CAS	login
		<b>ENTPersonProfils</b> (*)	Profils associés (Catégories de personnes)	<b>categories</b> (*)
		<b>ENTPersonDateNaissance</b> (*1)	Date de naissance	<b>dateNaissance</b> (*1)
	<b>ENTPersonCodePostal</b>	Code postal (Adresse personnelle)	codePostal	
Elèves	ENTEleve	<b>ENTEleveClasses</b>	Etablissements et classe associée	eleveClasses

\* L'attribut LDAP peut être utilisé en remplacement de la balise SAML.

(\*) attributs obligatoires dans tous les cas, ou (\*1) obligatoire uniquement pour les élèves

- La balise **categories** est obligatoire, elle permet de faire correspondre les utilisateurs aux Espaces de PRONOTE.net. Une table de correspondance est à remplir lors de l'installation de PRONOTEcas dans l'onglet Correspondances LDAP.
- Les balises **nom** et **prenom** sont obligatoires pour la fédération d'identité.
- La balise **dateNaissance** est obligatoire uniquement pour la fédération d'identité des élèves. Les deux formats supportés pour la date de naissance sont : « JJ/MM/AAAA » et « AAAA-MM-JJ ».
- La balise **codePostal** n'est pas obligatoire mais si vous la renseignez, elle doit être renseignée pour tous conformément aux données LDAP.
- La balise **eleveClasses**, qui ne concerne que les élèves, n'est pas obligatoire mais si vous la renseignez, elle doit être renseignée pour tous conformément aux données LDAP. Si plusieurs classes sont renseignées seule la première est utilisée.
- Les balises **user** ou **login**, si elles sont renseignées, seront utilisées lors des connections suivantes afin d'accélérer l'identification.

## 3 . Configuration du serveur CAS pour la diffusion des attributs

Les tests effectués sont basés sur les références suivantes :

- Serveur CAS version 3.1.1,
- Client CAS version 3.1.3,
- Protocole de validation du ticket CAS : SAML 1.1

### 3.1. Récupération des attributs dans LDAP

Par défaut, CAS n'envoie au service que le nom de l'utilisateur lors de la validation du ticket.

Pour ajouter des attributs LDAP il faut modifier le fichier .\WEB-INF\deployerConfigContext.xml

## Modification de «authenticationManager»

```
<bean id="authenticationManager"
class="org.jasig.cas.authentication.AuthenticationManagerImpl">
  <property name="credentialsToPrincipalResolvers">
    <list>
      <bean class="org.jasig.cas.authentication.principal.UsernamePasswordCredentials-
ToPrincipalResolver" >
        <property name="attributeRepository">
          <ref bean="attributeRepository" />
        </property>
      </bean>
    </list>
  </property>
  ...
</bean>
```

## Modification d' «attributeRepository»

```
<bean id="attributeRepository"
class="org.jasig.services.persondir.support.ldap.LdapPersonAttributeDao">
  <property name="baseDN" value="OU=xxxx,DC=xxxxxxxxxxxx,DC=xx" />
  <property name="query" value="(uid={0})" />

  <property name="contextSource" ref="contextSource" />

  <property name="ldapAttributesToPortalAttributes">
    <map>
      <entry key="sn" value="nom"/>
      <entry key="givenName" value="prenom" />
      <entry key="uid" value="user" />
      <entry key="ENTPersonLogin" value="login" />
      <entry key="ENTPersonProfils" value="categories" />
      <entry key="ENTPersonDateNaissance" value="dateNaissance" />
      <entry key="ENTPersonCodePostal" value="codePostal" />
      <entry key="ENTEleveClasses" value="eleveClasses" />
    </map>
  </property>
</bean>
```

La valeur de la propriété "baseDN" doit correspondre à la structure de votre LDAP.

Dans le cas où vous utilisez un Microsoft Active directory, vous devez remplacer "uid" par "sAMAccountName" dans la valeur de la propriété "query".

## 3.2. Filtre de données par service

### Modification de «serviceRegistryDao»

Il s'agit de retourner des attributs utilisateurs différents selon le service qui interroge le serveur CAS.

Pour autoriser les attributs par service, il faut ajouter le service aux listes "registeredServices" avec les attributs dans

la valeur de la propriété "allowedAttributes"

```
<bean id="serviceRegistryDao"
class="org.jasig.cas.services.InMemoryServiceRegistryDaoImpl">
  <property name="registeredServices">
    <list>
      <bean
        class="org.jasig.cas.services.RegisteredServiceImpl"
        p:id="1"
        p:description="All"
        p:serviceId="*://url.du.service/**"
        p:name="NomDuService"
        p:theme="default"
        p:allowedToProxy="true"
        p:enabled="true"
        p:ssoEnabled="true"
        p:anonymousAccess="false">

        <property name="allowedAttributes" value="nom,prenom,user, login ,cate-
        gorie,dateNaissance, codePostal, classe"/>
      </bean>
    </list>
  </property>
</bean>
```

### 3.3. Encodage UTF-8

#### Modification du descripteur de déploiement «web.xml»

Ajout d'un filtre dans le fichier «web.xml» sur la servlet du CAS pour forcer l'encodage en UTF-8 :

```
<filter>
  <filter-name>FiltreEncodage</filter-name>
  <filter-class>
    org.springframework.web.filter.CharacterEncodingFilter
  </filter-class>
  <init-param>
    <param-name>encoding</param-name>
    <param-value>UTF-8</param-value>
  </init-param>
  <init-param>
    <param-name>forceEncoding</param-name>
    <param-value>>true</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name> FiltreEncodage </filter-name>
  <url-pattern> /samlValidate </url-pattern>
</filter-mapping>
```

#### POSITION

Il faut positionner ce filtre en première position dans la liste des filtres.

