PRONOTE 2010
utilisation de PRONOTEcas

PRONOTEcas sert à interfacer PRONOTE.net à un ENT utilisant l'authentification avec CAS.

Ce manuel est destiné au gestionnaire de l'ENT.

Aucune assistance n'est assurée par Index Education auprès des établissements pour l'installation de ce module.

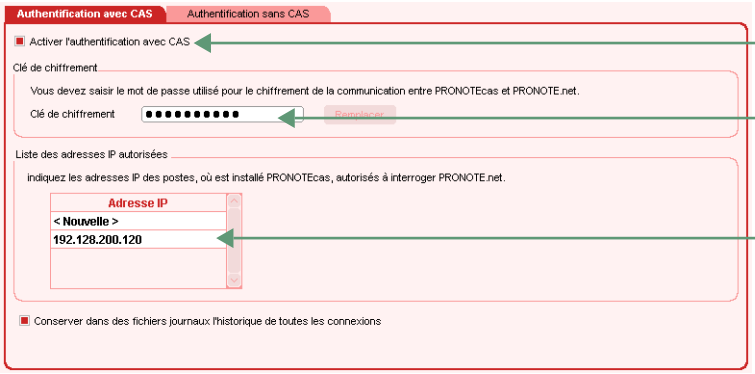
INDEX-EDUCATION.COM
NOS LOGICIELS FONT AVANCER L'ÉCOLE

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

PRONOTE.net doit être configuré comme ci-dessous.



1 L'autentification avec CAS doit être activée.

2 La clé de chiffrement doit être la même que celle saisie dans l'onglet Sécurité de PRONOTEcas *(voir page 2)*.

3 La (ou les) adresse(s) IP du ou des postes où est installé PRONOTEcas doivent être renseignées.

2 - Configuration de PRONOTEcas

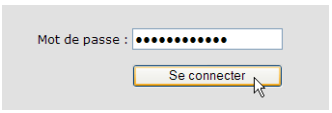
Vous devez disposer d'un serveur Tomcat version 5.5 et de JRE à partir de la version 1.5 - 016.
Nous conseillons aussi un protocole https pour sécuriser au maximum les communication réseau.

>> Installation de PRONOTEcas

1. Sur la page **Téléchargement > PRONOTE** du site Internet **www.index-education.com**, cliquez sur **PRONOTEcas**.
2. Installer un seul PRONOTEcas pour tous les établissements.
3. Choisissez le répertoire de destination du fichier ***.war**, il s'agit du répertoire **/webapps** de la machine où est installée le serveur Tomcat.

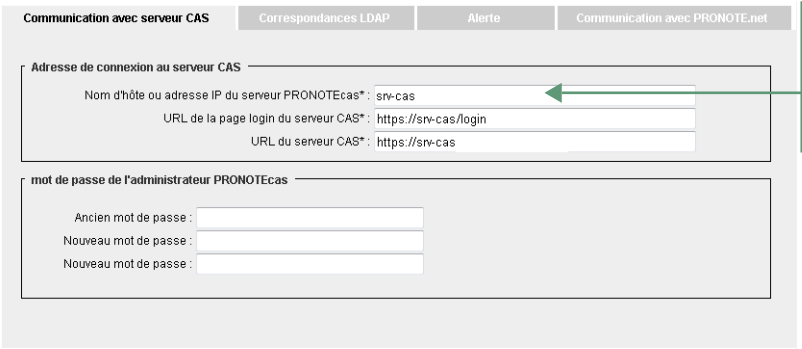
>> Première connexion à PRONOTEcas

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



Modifier le mot de passe administrateur

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



1 Renseignez toutes les informations nécessaires à la communication entre PRONOTEcas et le serveur cas.

Le protocole HTTPS obligatoire.

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.

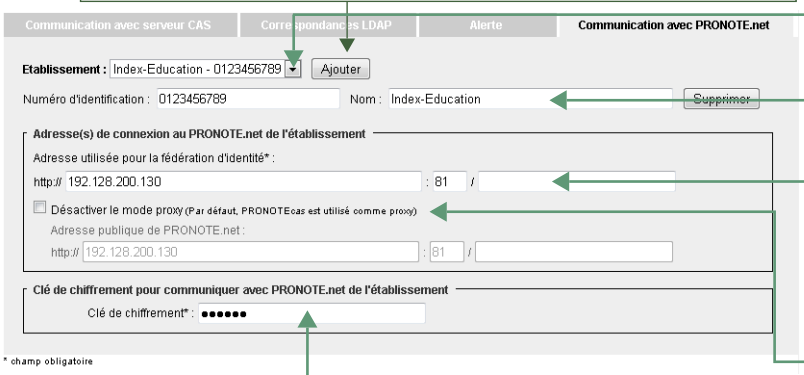
Le bouton **Valider** ne devient actif que lorsque vous avez rempli tous les champs obligatoires de configuration dans les onglets **Communication avec le serveur CAS** et **Communication avec PRONOTE.net**. Pour mieux les distinguer, ils sont marqués d'un astérisque (*).

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

Configurer la communication avec PRONOTE.net

L'onglet **Communication avec PRONOTE.net** permet de configurer, pour chaque établissement, la connexion à PRONOTE.net.

Le bouton **Ajouter** permet de créer un nouvel établissement.



1 Choisissez un établissement.

2 Saisissez son N° et son nom.

3 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).

4 Par défaut PRONOTEcas est utilisé comme proxy et relaie aussi les communications entre les espaces et PRONOTE.net.
En désactivant ce mode vous permettez une communication directe à PRONOTE.net. De ce fait, vous devez renseigner son adresse publique.

5 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.

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[1]. Cependant, chaque projet ENT est libre de définir des valeurs différentes pour l'attribut "ENTPersonProfils".

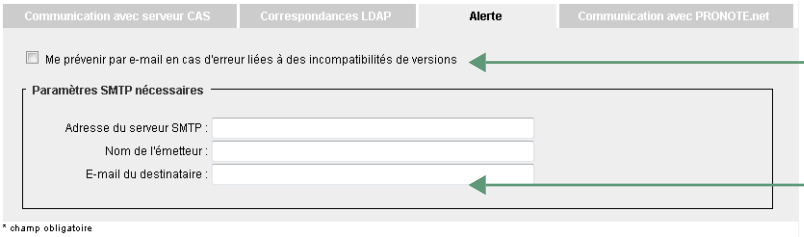
Si votre ENT a défini des valeurs particulières pour l'attribut "ENTPersonProfils", vous devez l'indiquer via cet écran de paramétrage.

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

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

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.



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

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

>> Connexions suivantes

Une fois la configuration effectuée, connectez-vous sur : **URL_DeLaMachineAbritantLeServeurTomcat/NomDuFichierWar/admin.htm**.
En tant qu'administrateur de PRONOTEcas, vous devez vous authentifier auprès de CAS pour accéder à PRONOTEcas.

>> Accès à PRONOTE.net à travers PRONOTEcas pour un établissement

La connexion se fait par l'adresse suivante : **URL_DeLaMachineAbritantLeServeurTomcat/NomDuFichierWar/?id=N°Identification**

30 avri rlr2i7. l7 2i . lr2i7 .7 i i r.7 7 7 r. 7 . 7 . 7 .7 i i r.7 7 2 .i l7 ri r 7 7 . r2i730 7 30 avril 2007.

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'éxécution 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 A partir de son navigateur, l'utilisateur connecté à l'ENT s'adresse à PRONOTEcas pour se connecter à PRONOTE.net.

2 PRONOTEcas répond au navigateur de s'adresser au serveur CAS et lui en donne l'adresse. Si l'utilisateur n'est pas déjà identifié sur le serveur, il devra saisir son identifiant et son mot de passe.

3 Le serveur CAS vérifie alors l'identité de l'utilisateur dans l'annuaire LDAP :
- si le LDAP n'authentifie pas l'utilisateur un message d'échec est envoyé à l'utilisateur sur l'ENT,
- si le LDAP authentifie l'utilisateur, le serveur CAS génère un «ticket CAS» et extrait de l'annuaire LDAP tous les attributs nécessaires à PRONOTE.net pour reconnaître l'utilisateur.

Un «ticket CAS» est une clé chiffrée à usage unique.

4 L'identifiant de l'utilisateur et son «ticket CAS» sont transmis à PRONOTEcas, grâce à une redirection du navigateur.

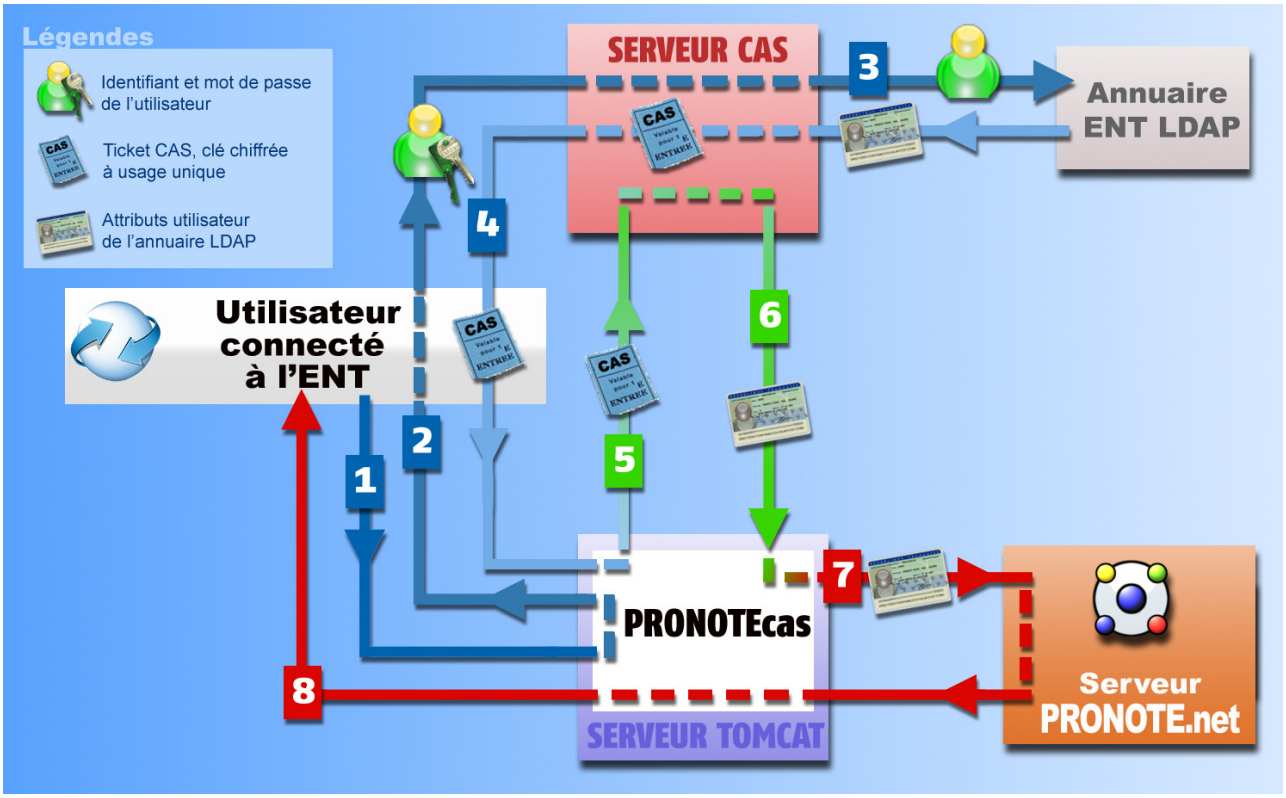
5 PRONOTEcas donne au serveur CAS le ticket de l'utilisateur.

6 Le serveur CAS renvoie à PRONOTEcas les attributs utilisateur de l'annuaire LDAP correspondant à ce ticket.

7 PRONOTEcas transmet ces attributs à PRONOTE.net qui peut alors identifier l'utilisateur dans son propre système de base de données.

8 L'utilisateur reçoit alors par l'intermédiaire de PRONOTEcas l'autorisation de se connecter à PRONOTE.net.

Si PRONOTEcas est configuré comme un proxy, il relaie les informations, entre PRONOTE.net et le navigateur, durant toute la session, dans le cas contraire, il permet à PRONOTE.net de communiquer directement avec 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	**sn** (*)	Nom d'usage	**nom** (*)
	inetOrgPerson	**givenName** (*)	Prénom usuel	**prenom** (*)
	ENTPerson	ENTPersonLogin	Identifiant CAS	login
		ENTPersonProfils (*)	Profils associés (Catégories de personnes)	**categories** (*)
		ENTPersonDateNaissance (*1)	Date de naissance	**dateNaissance** (*1)
		ENTPersonCodePostal	Code postal (Adresse personnelle)	codePostal
Elèves	ENTEleve	ENTEleveClasses	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.
- La balise **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

>> 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>
            …
```

Modification d' «attributeRepository»

```
<bean id="attributeRepository"
class="org.jasig.services.persondir.support.ldap.LdapPersonAttributeDao">
<property name="baseDN" value="OU=xxxx,DC=xxxxxxxxxx,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".

>> 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-
gories,dateNaissance, codePostal, classe"/>
            </bean>
         </list>
      </property>
</bean>
```

>> 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. Il faut positionner ce

filtre en première position dans la liste des filtres.

```
<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>
```