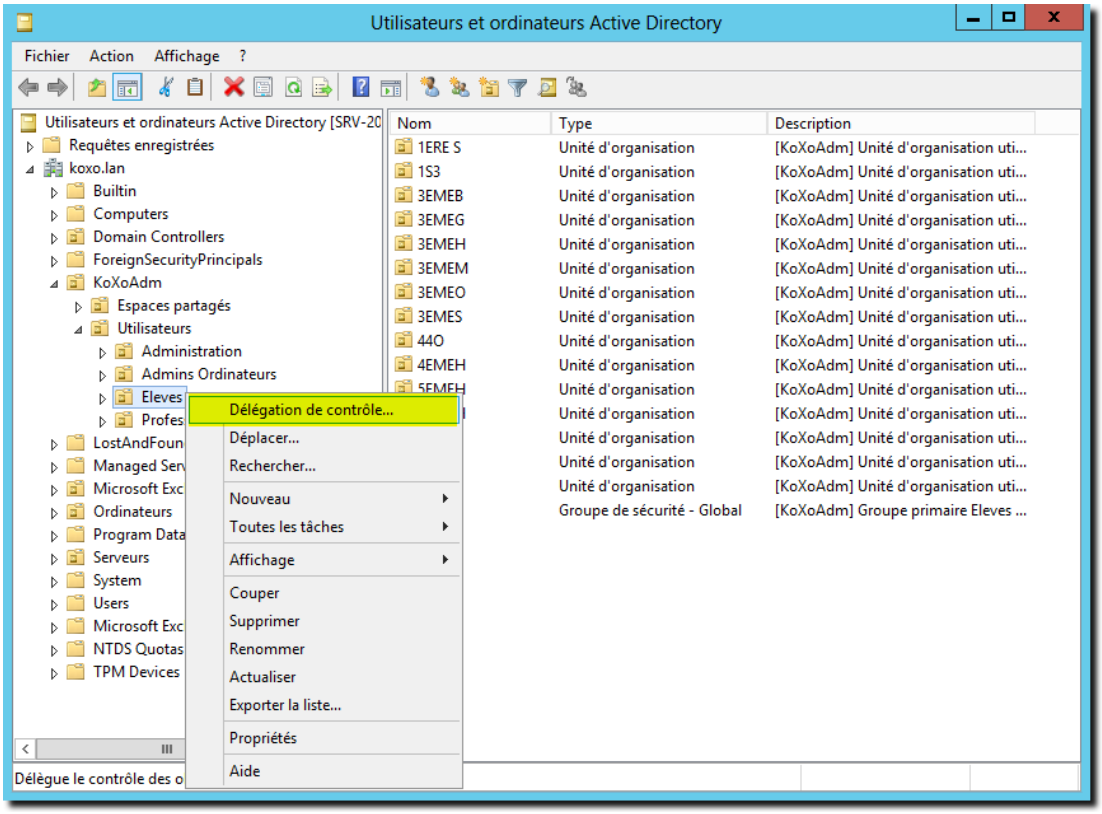
KOXO PASSWORDS

1 – Avant-propos

La délégation du changement des mots de passe est une opération simple à réaliser dans un domaine Microsoft. Cette opération permet de décharger l'administrateur et se consacrer à des tâches plus techniques. Il existe de nombreuses solutions s'appuyant sur un service installé sur le serveur et généralement un client accessible dans un partage du même serveur, ce mécanisme reproduit le mécanisme natif du serveur Microsoft en **négligeant la sécurité**, le mot de passe est envoyé en clair ou de manière réversible sur le réseau. La solution décrite ici respecte pleinement la sécurité car elle utilise les mécanismes natifs de Windows. Afin de ne pas avoir à installer les outils d'administrations sur tous les postes, un exécutable complet est proposé.

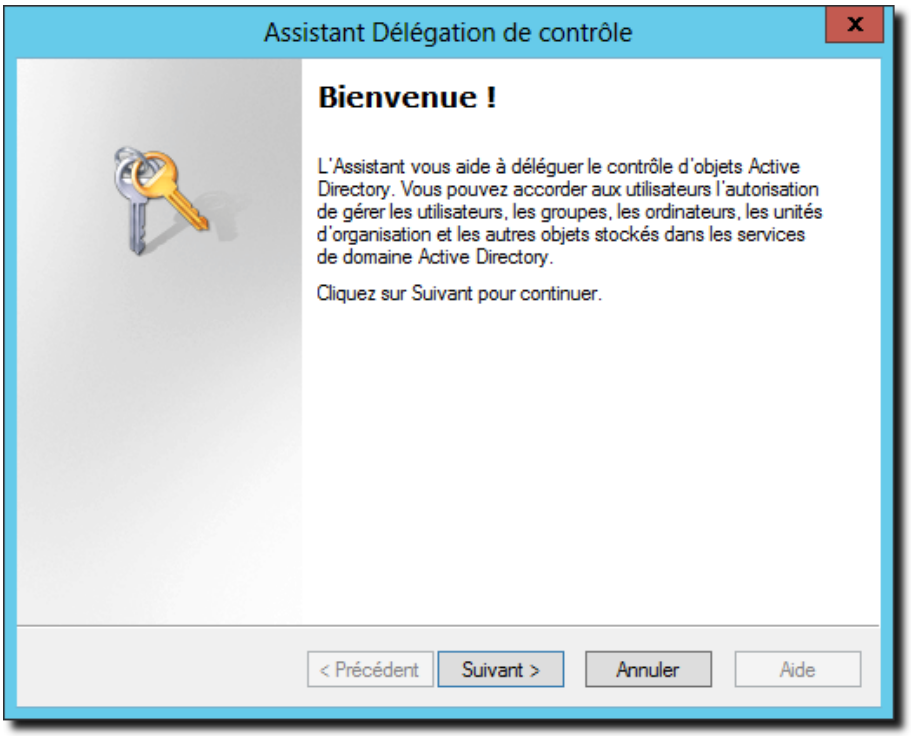
2 – Délégation Active Directory

L'exemple choisi est le cas d'un établissement scolaire ou l'on voudrait que les professeurs puissent changer le mot de passe des élèves. Il faut d'abord lancer la console MMC « **Utilisateurs et Ordinateurs Active Directory** », et se positionner sur l'unité d'organisation « **racine** » de la catégorie de personnes à gérer (ici les élèves) :



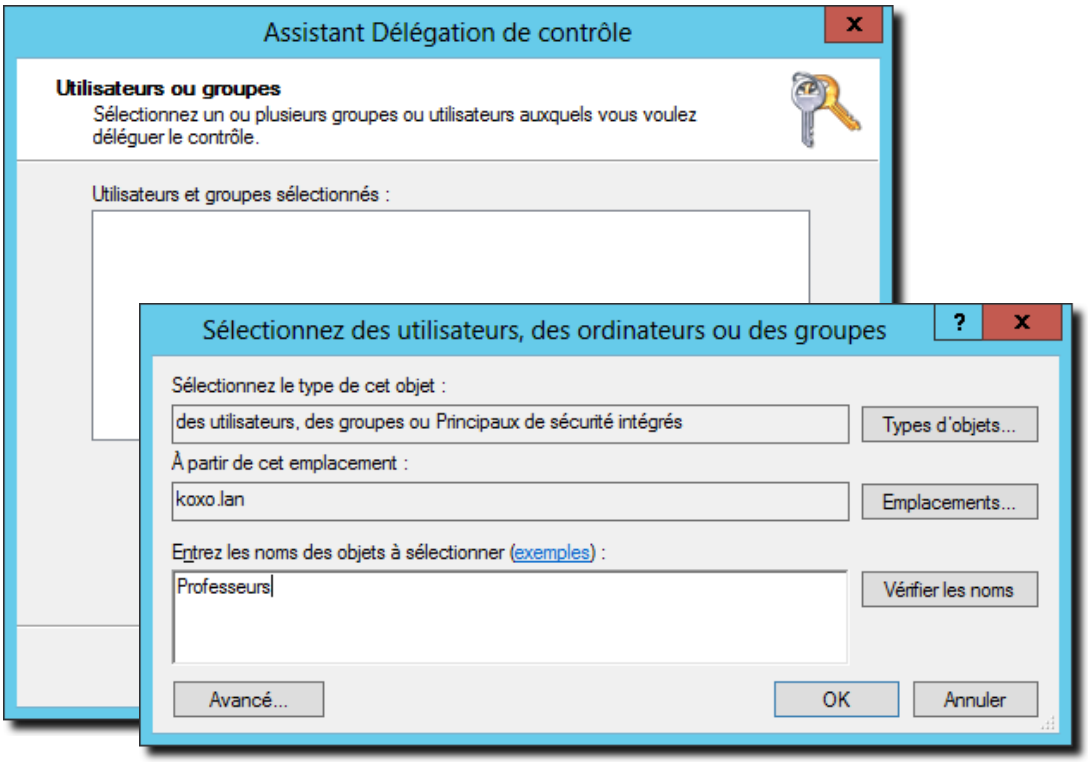
Délégation de contrôle

Un assistant apparaît alors :



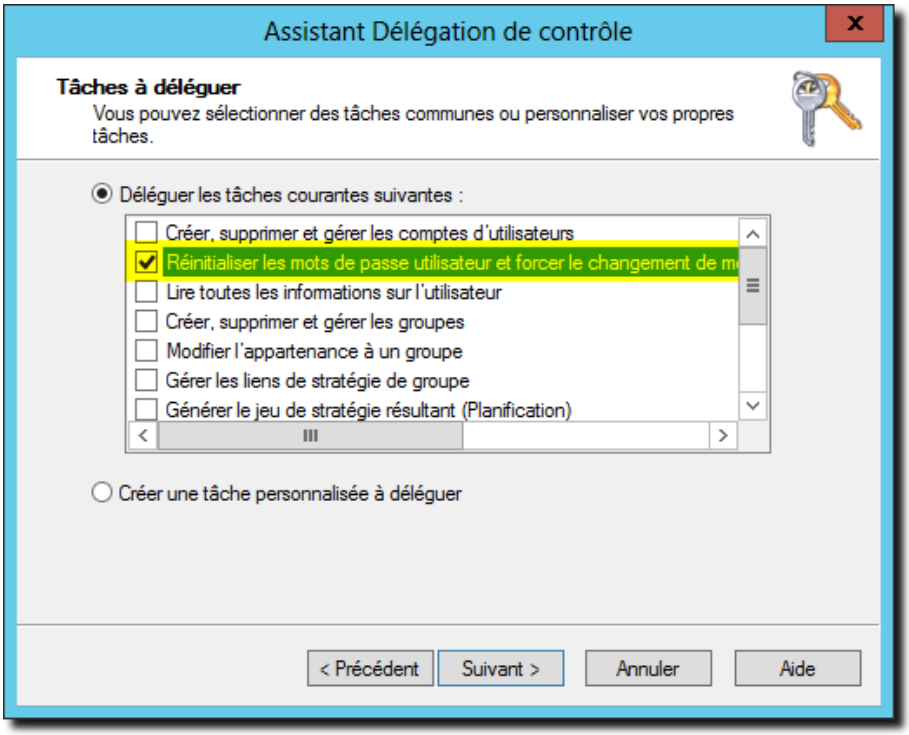
Assistant de délégation de contrôle

Il faut indiquer ici les utilisateurs et groupes qui pourront changer le mot de passes des utilisateurs de l'unité dorganisation « **Eleves** ».

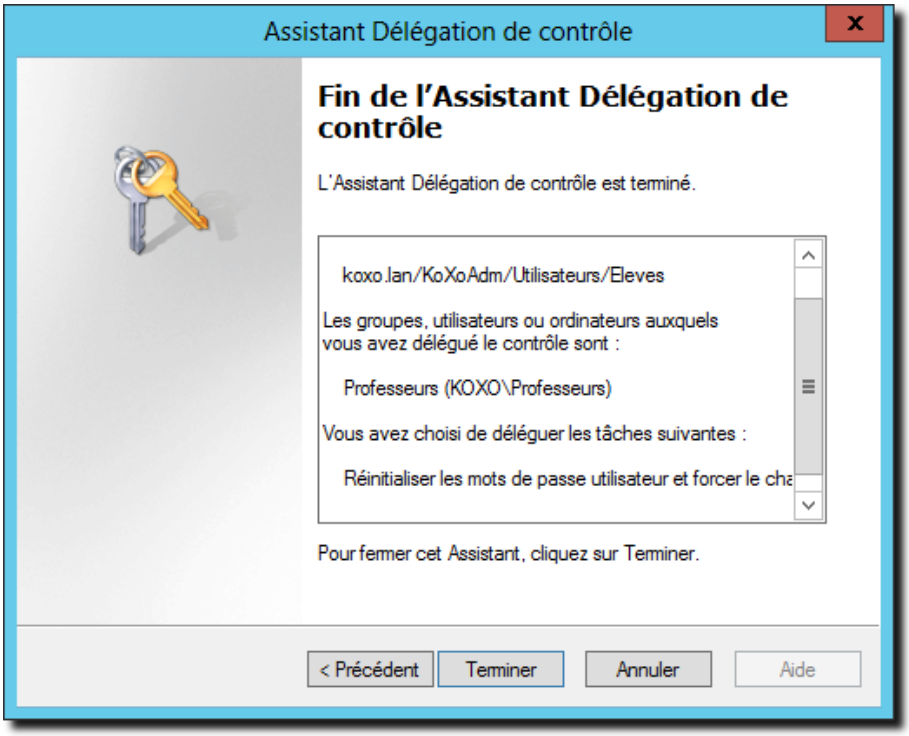


Choix des Utilisateurs et groupes

On indique ensuite que l'on souhaite « **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe** » :



Tâches à déléguer



Fin de l'opération

3 – Installation de KoXo Passwords

L'outil KoXo Passwords n'a pas besoin d'être installé et ne demande pas de librairies supplémentaires, il suffit de le recopier dans un dossier réseau accessible des personnes concernées. (Il est préférable que ça soit une ressource en accès en lecture seule). Afin d'accélérer la recherche des utilisateurs, il vaut mieux préconfigurer un fichier « **KoXoPasswords.xml** » (placé dans le même dossier que l'exécutable) afin d'indiquer le chemin de départ de la recherche des utilisateurs. Si ce fichier n'est pas présent il est généré automatiquement au premier lancement, il suffira donc de le compléter. Un exemple de fichier peut être généré en lançant KoXo Passwords avec le commutateur « **/WriteConfig** ».

Exemple de fichier initial (mono site) :

```
<?xml version="1.0" encoding="UTF-8"?>
<CONFIG_Passwords3>
  <NetworkSettings>
    <LogonServer></LogonServer>
    <!--Enter a value to override logon server detection-->
    <LDAPPath>OU=Elèves,OU=Utilisateurs,OU=KoXoAdm,%LDAP_DOMAIN%</LDAPPath>
    <LDAPUserFilter>(&amp;(objectClass=user)(|(sAMAccountName=%s)(givenName=%s)(sn=%s)))</LDAPUserFilter>
    <LDAPGroupFilter>(&amp;(objectClass=group)(|(sAMAccountName=%s)(name=%s)))</LDAPGroupFilter>
  </NetworkSettings>
  <PasswordSettings>
    <Algorithm>12</Algorithm>
    <!--Password generator Algorithms :-->
    <!--1 - Phonemes-->
    <!--2 - Numbers-->
    <!--3 - Letters-->
    <!--4 - digits and Letters-->
    <!--5 - digits and Letters Uppercase/Lowercase-->
    <!--6 - digits and Letters Uppercase/Lowercase and Special chars-->
    <!--7 - Phonemes Uppercase/Lowercase-->
    <!--8 - Phonemes first letter Uppercase-->
    <!--9 - A least a lowercase letter, an uppercase letter and a number-->
    <!--10- A least a lowercase letter, an uppercase letter, a number ans a spec. char-->
    <!--11- Pseudo-complex (8 chars phonemes with upp + number + 1 special char)-->
    <!--12- Pseudo-complex like Office 365 (8 chars : 1 up + 3 low + 4 digits)-->
    <!--13- Pseudo-complex with 2 phonemes (with uppercase) and 4 digits-->
    <!--14- Pseudo-complex 9 chars (1 up + 3 low + 1 spec. char + 4 digits)-->
    <!--15- 12 chars (3 phonèmes (8 chars) + 1 spec. char + 3 digits)-->
    <!--99- Formula (Default : #UPPER1{#PHONEME{2}}#RANDOM{2}#SPECIAL_CHAR{1})-->
    <Length>8</Length>
    <EnhanceReadability>-1</EnhanceReadability>
    <UserMustChangePassword>-1</UserMustChangePassword>
    <HideChangePassword>0</HideChangePassword>
    <Formula>#UPPER1{#PHONEME{2}}#RANDOM{1}#SPECIAL_CHAR{1}</Formula>
  </PasswordSettings>
  <Miscellanous>
    <Company></Company>
    <!--Enter a value to override user's AD value-->
    <Year>
      <Value></Value>
      <!--Value is not used if autodetection is enabled-->
      <CalendarType>0</CalendarType>
      <!--Accepted values : 0=School year, -1=Calendar year-->
      <Autodetection>-1</Autodetection>
      <SchoolFirstDay>1</SchoolFirstDay>
      <SchoolFirstMonth>8</SchoolFirstMonth>
    </Year>
    <Variables>
      <Variable>
        <Name>%WEBMAIL_SERVER%</Name>
        <Value>http://mail.office365.com</Value>
      </Variable>
    </Variables>
    <Printing>
      <OffsetX>0</OffsetX>
      <OffsetY>0</OffsetY>
      <LabelsTemplate>LabelsTemplate.xml</LabelsTemplate>
    </Printing>
    <Style>Office2019White</Style>
    <!--Accepted values : Office2019White, Office2019Gray, Office2010Blue, Office2010Silver, Windows7, Windows8, Windows10-->
  </Miscellanous>
</CONFIG_Passwords3>
```

Indiquer ici un éventuel serveur de logon, sinon le serveur est détecté.

Modifier ici le chemin LDAP des utilisateurs dont le mot de passe pourra être changé

Indiquer ici votre stratégie de mots de pass

Le nom de la société qui est affiché dans le titre de la fiche

Les étiquettes peuvent avoir besoin de déterminer l'année en cours

Indiquer ici les variables personnalisées nécessaires aux étiquettes

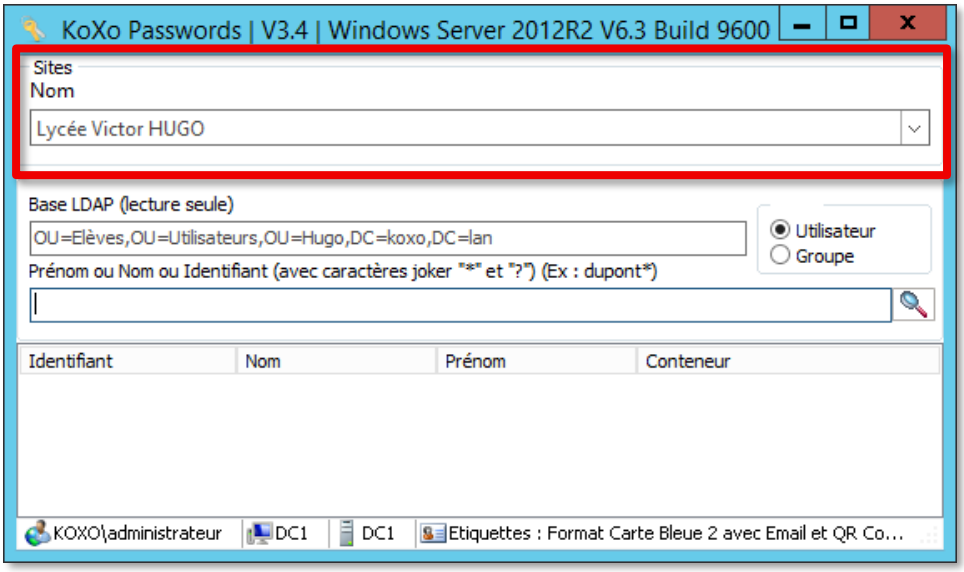
Nom du modèle d'étiquettes

Exemple de fichier initial (multisite) :

```
<?xml version="1.0" encoding="UTF-8"?>
<CONFIG_Passwords3>
  <NetworkSettings>
    <LogonServer>DC1</LogonServer>
    <!--Enter a value to override logon server detection-->
    <LDAPUserFilter>(&amp;(objectClass=user)(|(sAMAccountName=%s)(givenName=%s)(sn=%s)))</LDAPUserFilter>
    <LDAPGroupFilter>(&amp;(objectClass=group)(|(sAMAccountName=%s)(name=%s)))</LDAPGroupFilter>
  </NetworkSettings>
  <Sites>
    <Site>
      <Name>Lycée Victor HUGO</Name>
      <LDAPPath>OU=Elèves,OU=Utilisateurs,OU=Hugo,%LDAP_DOMAIN%</LDAPPath>
    </Site>
    <Site>
      <Name>Lycée Molière</Name>
      <LDAPPath>OU=Elèves,OU=Utilisateurs,OU=Molière,%LDAP_DOMAIN%</LDAPPath>
    </Site>
  </Sites>
...................
...................
</CONFIG_Passwords3>
```

Balise « **Sites** »

Créer une balise « **Site** » par site, y déclarer le chemin LDAP et le nom à afficher dans l'interface. Si l'utilisateur n'a pas d'attribut « **company** » cette valeur est alors utilisée par la variable « **%COMPANY%** ».



Les options de ligne de commande :

Option	Signification
/WriteConfig	Permet de réaliser un exemple de fichier de configuration, à modifier à sa convenance.
/Site=x **/Site="Nom du site"**	On peut indiquer le site aves son numéro (à partir de 1) ou avec son nom (Exemple : /Site="Lycée Victor HUGO"
/LockSite	La boite déroulante de sélection de sites est verrouillée.

Attention : En plus du modèle d'étiquettes il faudra probablement créer un dossier « Files » et y placer les fichiers référencés dans le modèle. (Exemple : « Office365.bmp »).

Il est possible de pré cocher la boîte à cocher pour imposer le changement de mot de passe via « **UserMustChangePassword** » et même de cacher cette boîte à cocher via « **HideChangePassword** ».

Lorsque l'on décide générer automatiquement le mot de passe est généré en fonction de trois paramètres : algorithme, longueur et l'amélioration de la lisibilité du mot de passe (les I, i, 1, O,0 sont évités dans certains algorithmes).

Enfin quelques modèles de styles sont proposés (Office 2010, 2019, etc.), le style « **Office 2019 Blanc** » est celui qui est proposé par défaut.

Algorithmes : Valeurs acceptées

1. Phonèmes
2. Chiffres
3. Lettres
4. Chiffres et Lettres
5. Chiffres et Lettres Maj./Min.
6. Chiffres et Lettres Maj./Min. et Caractère spéciaux
7. Phonèmes Maj./Min
8. Phonèmes première lettre en Maj.
9. Au moins une minuscule, une majuscule et un chiffre
10. Au moins une minuscule, une majuscule, un chiffre et un caractère spécial
11. Pseudo complexe (8 car. phonèmes avec maj. + chiffre + caractère spécial)
12. Pseudo complexe style Office 365 (8 car. : 1 maj + 3 min+ 4 chiffres)
13. Pseudo complexe avec 2 phonèmes (avec majuscule) et 4 chiffres maxi
14. Pseudo complexe 9 car. (1 maj + 3 min+ 1 car. spécial + 4 chiffres)
15. 12 caractères (3 phonèmes (8 caractères) + 1 car spécial + 3 chiffres)
99. Utilisation d'une formule (Défaut : `#UPPER1{#PHONEME{2}}#RANDOM{1}#SPECIAL_CHAR{1}`).

N.B. : Les algorithmes sont inspirés de ceux de KoXo Administrator

Styles : Valeurs acceptées :

- Office2019White
- Office2019Gray
- Office2010Blue
- Office2010Silver
- Office2010Black
- Windows7
- Windows8
- Windows10

Les variables pouvant être utilisées dans les étiquettes :

Variables Globales :

- %LOGON_SERVER% → Serveur de Logon
- %LAUNCHING_PATH% → Chemin de lancement de l'application
- %SOCIETY%, %COMPANY%, %COMPANY_NAME% → Nom de la société, établissement
- %VERSION% → Version du logiciel
- %COPYRIGHT% → Copyright
- %WEB_SITE% → http://www.koxo.net
- %YEAR% → Année d'utilisation
- %NETBIOS_DOMAIN%, %DNS_DOMAIN%, %LDAP_DOMAIN% → Domaine
- %DATE%, %LONG_DATE%, %TIME%, %LONG_TIME% → Date et heure courante
- %TAB% → Tabulation (Valeur ASCCI : « $09 »)
- %CRLF% → Séquence « $0D$0A »

Variables de groupes :

- %PRIMARY_GROUP% → Nom de groupe principal
- %PRIMARYGROUP% → Nom de groupe principal sans espaces
- %SECONDARY_GROUP% → Nom du sous-groupe
- %SECONDARYGROUP% → Nom du sous-groupe sans espaces

Variables de l'utilisateur :

- %USER_FQDN% → Nom LDAP (distinguishedName)
- %TITLE% → Titre civilité (personalTitle)
- %USER_TITLE% → Titre civilité (personalTitle)
- %USER_FUNCTION% → Fonction (title)
- %USER_ID% → Identifiant (sAMAccountName)
- %USER_NAME% ou %USER_LAST_NAME% → Nom (sn)
- %USER_FIRST_NAME% → Prénom (givenName)
- %USER_DISPLAY_NAME% → Nom affiché (displayName)
- %USER_PASSWORD% → Mot de passe (password)
- %USER_EMAIL% → Adresse email (mail)
- %USER_OTHER_MAILBOXES% → Autres boîtes aux lettres (otherMailbox)
- %USER_UPN% → Nom d'ouverture de session (userPrincipalName)
- %USER_INITIALS% → Initiales (initials)
- %USER_PHONE% → Téléphone (phone)
- %USER_MOBILE_PHONE% → Téléphone mobile (mobile)
- %USER_FAX_NUMBER% → Fax (facsimileTelephoneNumber)
- %USER_UNIQUE_ID% → Numéro de l'employé (employeeNumber)
- %USER_WEB_PAGE% → Page web (wWWHomePage)
- %USER_ PAGER% → Numéro du Pager aussi appelé bipeur (pager) (Les modèles de KoXo Administrator y stockent la date de naissance de l'utilisateur).
- %USER_DEPARTMENT% → Département ou service (departement)

Fonctions :

- #LOWER{...} → Minuscules
- #LOWER_ACC{...} → Minuscules
- #UPPER{...} → Majuscules
- #UPPER1{...} → Premier caractère en majuscule
- #FIRSTLETTER{...} → Première lettre
- #TRIM{...} → Enlève les espaces
- #TRIMR{...} → Enlève les espaces à droite
- #TRIML{...} → Enlève les espaces à gauche
- #BOOL{...} → Renvoie la valeur booléenne
- #REMOVE_SPACE{...} → Enlève les espaces
- #REMOVE_ACC{...} → Enlève les accents
- #CONV_SPACE{...} → Convertit les espaces en « _ »
- #DOS_ACC{...} → Convertit les accents DOS
- #INITIALS{...} → Renvoie les initiales
- #EMAIL_PREFIX{...} → Préfixe de l'adresse email
- #EMAIL_SUFFIX{...} → Suffixe de l'adresse email
- #HEX{...} → Chaine hexadécimale
- #BASE64{...} → Encodage en Base 64
- #MD5{...} → Hash MD5
- #MD5_BASE64{...} → Hash MD5 encodé en Base 64
- #SHA1{...} → Hash SHA1
- #SHA1_BASE64{...} → Hash SHA1 encodé en Base 64
- #SHA2{...} → Hash SHA2
- #SHA2_BASE64{...} → Hash SHA2 encodé en Base 64
- #CODE25{...} → Encodage Code 2 parmi 5
- #CODE39{...} → Encodage Code 3 parmi 9
- #CODE128{...} → Encodage Code 128
- #EAN13{...} → Encodage Code EAN13
- #RANDOM{…} → Génère un nombre aléatoire de « n » chiffres. Avec 8 chiffres au maximum avec 2 fois le même chiffre au maximum.
- #PHONEME{…} → Génère « n » phonèmes de 3 lettres.
- #SPECIAL_CHAR{…} → Génère « n » caractères spéciaux (=-+*/\()%_&#$@,:.!?[]{}&<>%).

Pour davantage de précisions sur ces fonctions, se reporter au manuel de KoXo Administrator.

Ordre de traitement des variables :

Le traitement est effectué comme suit :

1. Variables globales
2. Variables de l'utilisateur
3. Variables personnelles
4. Fonctions