Mixed mode authentication enables users to sign in to your website using both Windows Active Directory authentication and standard forms authentication.

**Forms and AD user name conflicts**

Active Directory users cannot authenticate if an existing forms user has the same user name (only the *common name* of the AD user is processed, i.e. without the domain component). In these cases, the system cannot create an account for the AD user. You can avoid these conflicts by renaming the existing forms user.

When a user signs in using Active Directory credentials for the first time, the system automatically creates a matching user account in the Kentico database and also imports the user's domain groups as roles. The imported roles do ***not*** authorize the users to perform any actions in Kentico by default. You need to configure permissions and UI personalization settings for the imported roles manually if you wish to use them.

**Disabling the automatic role import**

If you wish to disable the automatic import of user domain groups as roles in Kentico, add the following key to the */configuration/appSettings* section of your project's web.config file:

```
<add key="CMSImportWindowsRoles" value="false" />
```

## Prerequisites

For mixed mode authentication to work, the application must be able to access the following attributes of user objects in Active Directory (i.e. the attributes cannot be protected or confidential):

- **memberof**
- **userAccountControl**

## Configuring mixed authentication

To enable mixed authentication mode:

1. Edit your application's *web.config* file.
2. Make sure that the **mode** attribute of the **<authentication>** element in the <*system.web*> section is set to **Forms** (this is the default value for Kentico projects):

```
<authentication mode="Forms">
```

3. Add the LDAP connection string of your Active Directory service into the **configuration/connectionStrings** section:

```
<connectionStrings>
  ...
  <add name="CMSADConnectionString" connectionString="<LDAP connection string>" />
</connectionStrings>
```

- Replace the <*LDAP connection string*> text in the code above with the actual connection string. Enter it according to the following format:

```
LDAP://mydomain.example.com/DC=mydomain,DC=example,DC=com
```

The first part is the full domain. In the second part, the same domain is divided into DC (domain component) units.

4. Modify the **membership** and **roleManager** elements under the **configuration/system.web** section according to the following:

```
<membership defaultProvider="CMSProvider" userIsOnlineTimeWindow="30">
  <providers>
    <clear/>
         <add name="CMSProvider" type="CMS.MembershipProvider.
CMSMembershipProvider, CMS.MembershipProvider" connectionStringName="
CMSConnectionString" enablePasswordRetrieval="false" enablePasswordReset="true"
requiresQuestionAndAnswer="false" requiresUniqueEmail="true" passwordFormat="Hashed"
/>
    <add name="CMSADProvider" type="CMS.MembershipProvider.CMSADMembershipProvider,
CMS.MembershipProvider" connectionStringName="CMSADConnectionString"
connectionUsername="username" connectionPassword="password" />
  </providers>
</membership>
```

```
<roleManager defaultProvider="CMSRoleProvider" enabled="true" cacheRolesInCookie="
true" cookieName=".ASPROLES" cookieTimeout="30" cookiePath="/" cookieRequireSSL="
false" cookieSlidingExpiration="true" cookieProtection="All">
  <providers>
    <clear/>
         <add name="CMSRoleProvider" type="CMS.MembershipProvider.CMSRoleProvider,
CMS.MembershipProvider" connectionStringName="CMSConnectionString" applicationName="
SampleApplication" writeExceptionsToEventLog="false"/>
         <add name="CMSADRoleProvider" type="CMS.MembershipProvider.
CMSADRoleProvider, CMS.MembershipProvider" connectionStringName="
CMSADConnectionString" connectionUsername="username" connectionPassword="password"
/>
  </providers>
</roleManager>
```

- Replace the following values:
  - **username** – the user name of an Active Directory account that has read permissions for the required users and groups in your domain. Must include the fully qualified domain name, for example: ***office.example.com\johns***
  - **password** – the Active Directory password for the specified account

Users can now sign in with their Active Directory user name (without the domain) and password, or their standard Kentico user name and password.

You can also allow users to sign in using their full Active Directory user name (e.g. *MyName@office.example.com*) by adding the following key to the *appSettings* section of your *web.config* file:

```
<add key="CMSADDefaultMapUserName" value="userPrincipalName" />
```

**Password features not supported for Active Directory users**

The passwords of Active Directory users are stored externally and are not managed by Kentico. For these users, the system does not support any features related to password changes or requirements (for example Password reset, Password expiration, Password policies).