multiOTP® *AD Sync* configuration

This guide explains how to configure multiOTP Pro or Enterprise to synchronize users based on group membership between a Windows Active Directory server and multiOTP.

Setup of the AD sync process

In the **Configuration** menu, click on **External Server**.

Setting	What it is used for	Recommanded/example value
Active	To enable/disable sync. To force a sync, simply unchecked and click on **Apply**, then check and click on **Apply** again. This will force an AD sync.	Checked
Algorith for newly created users	What kind of token algorithm should be used when importing new users	TOTP
Prefix the OTP with PIN or AD/LDAP password	Should the OTP be prefixed by a PIN or AD password ?	Checked
Use AD/LDAP password instead of PIN for new users	Prefix PIN is the AD password by default	Checked
Force the value of "AD/LDAP password instead of PIN" during synchronization for all users	Force PIN to be AD password even on existing users	Unchecked
Accept expired AD/LDAP password	Should multiOTP accept AD password that are expired. For example, if uncheck, users are not able to connect VPN to change their password.	Checked
Enable multiple groups support for synchronized users		
Send provisioning by email to newly automatically created users	Check this box to send the provisioning information per email to any newly automatically created user. *The user must have an E-email address configured in the synchronized server before the first synchronization. No mail will be sent automatically after the creation of the user.*	Checked
Send scratch passwords list to newly automatically created users	Check this box to send the scratch passwords list per email to any newly automatically created user. *The user must have an E-email address configured in the synchronized server before the first synchronization. No mail will be sent automatically after the creation of the user.*	Unchecked
Deflect the information for new users to the administrative specific email address	Check this box to send all created emails to the administrative E-mail address instead of the user directly. *This is useful if you want to send physically the provisioning information by registered mail*	Unchecked

Server type	**Type of LDAP server**	**Microsoft Active Directory**
Server address	IP or FQDN of your local AD server	x.x.x.x
Backup server address	IP or FQDN of your second local AD server	y.y.y.y
Port	Port used for active directory service. *(standard is 389 for LDAP and 636 for LDAPS - LDAP with SSL)*	389
Base DN	Base DNS where to look for the users	DC=internal,DC=mycompany,DC=com
Users DN		
Groups(s) filtering	Comma separated list of groups containing the users to be synchronized. If the field is empty, not filter is applied. *(the first matching group will be the group of the user and will be returned as the Filter-Id (11) attribute by the RADIUS)*	A_Groupe,B_Groupe
Without2fa group(s) filter		
Network timeout	After this timeout, the backup server is contacted.	10
Search time limit	After this maximum time limit, the communication with the AD/LDAP server is closed, even if the job is not finished.	30
Synchronization interval	Interval to look for new/deleted users in AD	60
Synced account attribute	Attribute	
Delete unsynchronized accounts after	After x days, delete users that are not present in AD anymore. On each sync users remove from AD are disabled in multiOTP but not deleted.	30
Bind DN	Bind DN to connect to the AD/LDAP server	CN=sync,CN=Users,DC=internal ,DC=mycompany,DC=com
Password	Password to connect to the AD/LDAP server.	
Login name attribute	Login name attribute used in the AD/LDAP server. Default is *sAMAccountName*	
Group membership attribute	Group membership attribute used in the AD/LDAP server. Default is *memberof*	

Licence management during AD sync

During synchronization, users get a licence automatically until there is none left. If there is no licence left, the user is imported into multiOTP pour he stays disabled.