

## Setting up the LDAP tool

This article will outline how to use the LDAP tool which sits in the Sysadmin Panel from Claromentis 8.3+

This LDAP tool means you can connect your company Active directory to sync with your Claromentis intranet without the need for a technician to get involved, meaning any time you need to change what LDAP attributes are syncing or which groups are being pulled this can be done from within the intranet itself.

The first step is to go into the Sysadmin panel and from here the LDAP tab.

If this is the first time you are setting this up you will need to select the new connection option. You will then be shown the 5 steps to set this up as outlined below.

### Connection

In step 1 'Connection' you will need to input the following information:

A screenshot of the 'LDAP Connections' configuration interface. The title 'LDAP Connections' is at the top left. Below it is a green header bar with a checkmark and the text '1. Connection'. The main area contains five input fields, each with a red asterisk and an information icon to its right. The fields are: 'LDAP Server URL' with the value 'ldap://ad1.claromentis.net:389'; 'NetBIOS Name' with the value 'AD1'; 'Service Account DN' with the value 'AD1\connectiontest'; 'Service Account Password' with a masked password and a 'Change password' link; and 'Search Base DN' with the value 'DC=ad1,DC=claromentis,DC=net'. Below the fields is a purple 'Test Connection' button, a green checkmark with the text 'Connection OK!', a purple link 'show advanced settings...', and a purple 'Continue' button. At the bottom of the screen, a green header bar with a checkmark and the text '2. Directory Settings' is partially visible.

Image 1: Connection setting in the LDAP tool

**LDAP Server URL:** The URL must include the protocol (LDAP or LDAPS), LDAP server address and TCP port used for communication between Claromentis and the LDAP server. Eg. - ldap://ad1.claromentis.net:389

**NetBIOS Name:** First part of FQDN, for example for ad1.claromentis.net it would be AD1. The NetBIOS name should always be in upper case (A-Z), any lowercase characters will be converted to uppercase when saving.

**Service Account DN:** We recommend setting up a Claromentis specific Service Account that can be used to run all LDAP search queries. Claromentis only requires read access to the domain and therefore, in most cases, the fact that the Service Account is part of the 'Authenticated Users' group will provide sufficient access rights.

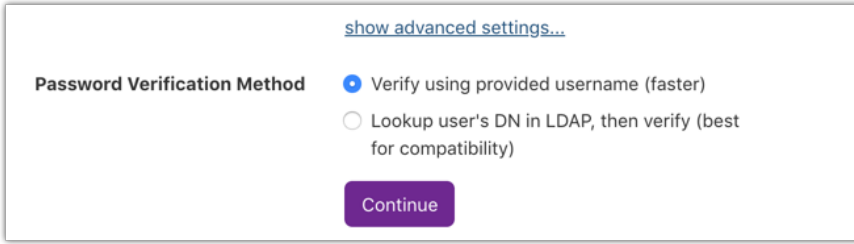
It's also recommended not to set a password expiry policy for this Service Account given that any LDAP user on Claromentis will be unable to login if this Service Account fails to authenticate with the LDAP server

**Service Account Password:** This is not stored in the system

**Search Base DN:** The DN (Distinguished Name) of the Search Base. This is the starting point used for any LDAP search query

Once you have input all the information you should be able to test the connection and get the tick with connection ok as shown in image 1.

The final stage in the connection settings is the advanced settings.



show advanced settings...

**Password Verification Method**

- Verify using provided username (faster)
- Lookup user's DN in LDAP, then verify (best for compatibility)

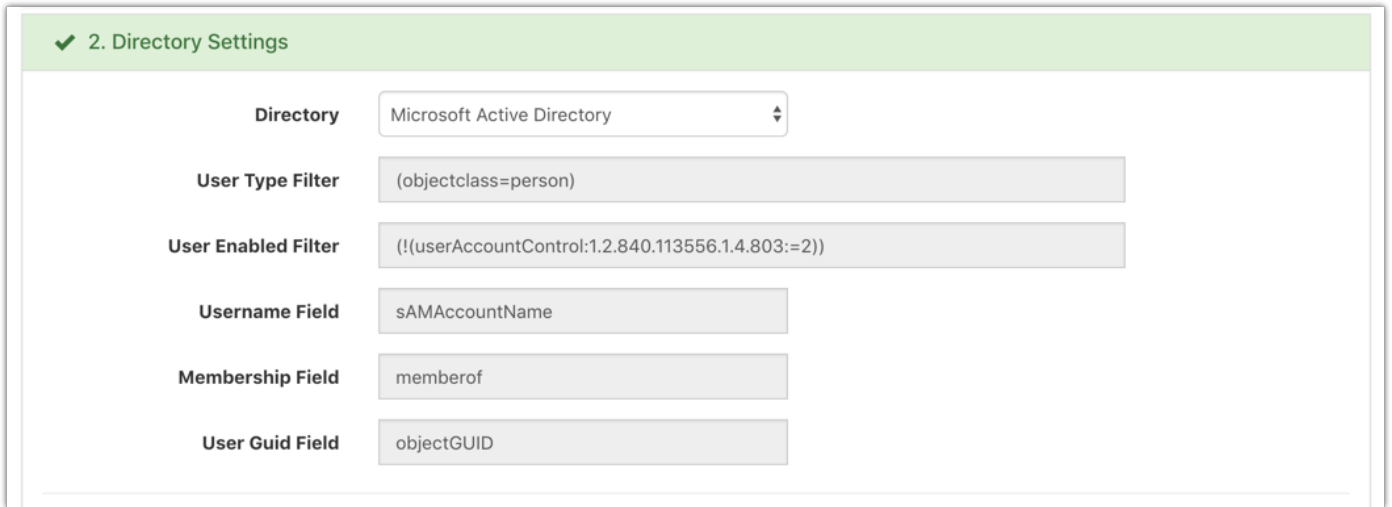
Continue

Image 2: Password verification method

This is to set the Password verification method, you will be able to select the best option for you. Once selected select continue.

### Directory Settings

You will then be able to move onto the second step the Directory Settings.



✓ 2. Directory Settings

**Directory** Microsoft Active Directory

**User Type Filter** (objectclass=person)

**User Enabled Filter** (!(userAccountControl:1.2.840.113556.1.4.803:=2))

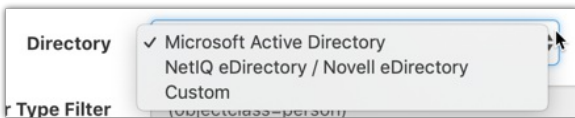
**Username Field** sAMAccountName

**Membership Field** memberof

**User Guid Field** objectGUID

Image 3: Directory Settings

You will first need to select your directory from the drop down.



Directory

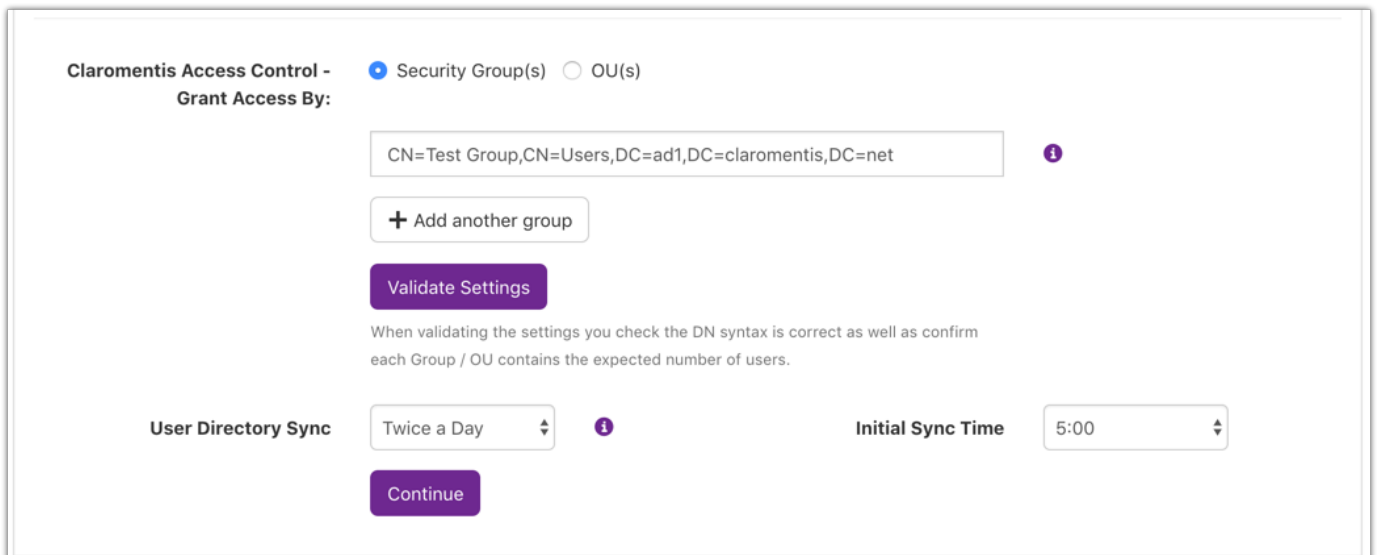
- ✓ Microsoft Active Directory
- NetIQ eDirectory / Novell eDirectory
- Custom

User Type Filter (objectclass=person)

Image 4: Directory Options

After this fill in the fields from your AD settings included in Image 3.

The second part of the Directory settings is the access control and setting up the sync as shown in image 4.



**Claromentis Access Control - Grant Access By:**

Security Group(s)  OU(s)

CN=Test Group,CN=Users,DC=ad1,DC=claromentis,DC=net ⓘ

+ Add another group

Validate Settings

When validating the settings you check the DN syntax is correct as well as confirm each Group / OU contains the expected number of users.

**User Directory Sync** Twice a Day ⓘ

**Initial Sync Time** 5:00

Continue

Image 5: Directory Settings cont.

You will be able to choose how Claromentis is given access and specify the OU using the DN format. Your user directory sync can be set up as a specific time and how often. The following options are given.

- Disabled
- Every Hour
- Twice a day
- Daily (Recommended)
- Weekly

Depending on what option you select you will be able to specify the initial sync time. Once complete select continue to move on to syncing the LDAP attributes which is outlined in this article - LDAP attributes article.

### User Groups

After you have synced the LDAP attributes you can move on to the group set up.

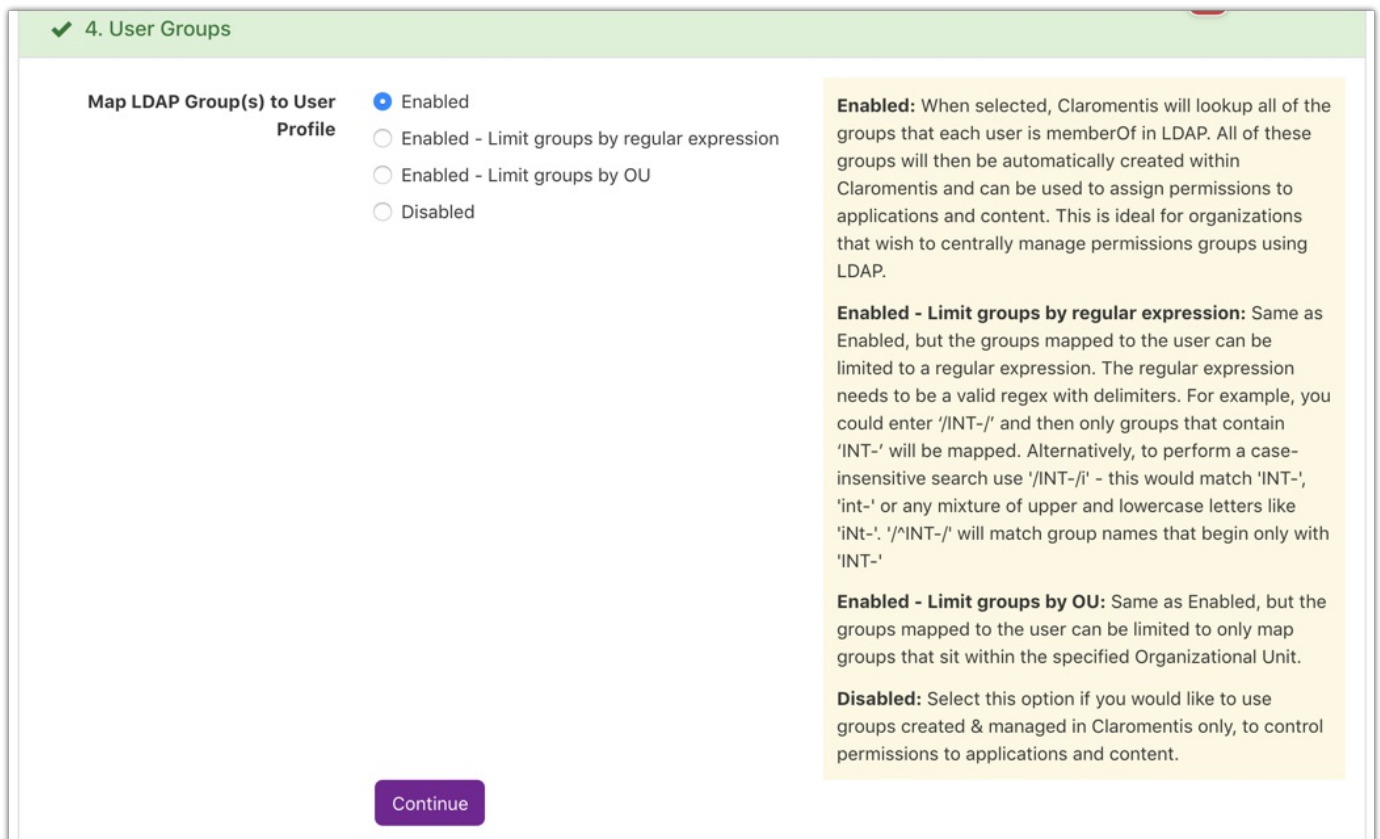


Image 6: User Groups

There are 4 options you have with the user sync, please read each option thoroughly to decide what syn will work best for you.

### Status

The final step in the LDAP tool configuration is to select the status this is weather you need to enable or disable the LDAP connection, this can be disable but the details remain if needed.

Once you have set everything correctly please click save in the bottom right hand corner to complete the setup.